A Novel Proactive Multi-secret Sharing Scheme

Bin Feng, Cheng Guo, Mingchu Li, and Zhihui Wang
(Corresponding author: Zhihui Wang)

School of Software Technology, Dalian University of Technology
No.8 Road, Jinzhou District, Dalian 116620, P. R. China
(Email: wangzhihui1017@gmail.com)
(Received Dec. 24, 2013; revised and accepted Jan. 16, 2015)

Abstract

A proactive secret sharing scheme is a method of sharing a secret among a set of participants. And, the corresponding shadows can be periodically renewed under the premise of never changing the shared secret. However, in the most existing proactive secret sharing schemes, only one secret can be shared during one secret sharing process. The proposed scheme describes PMSS, a new way to share multiple secrets with the proactive characteristic. In the proposed scheme, multiple secrets can be shared among many participants and shadows can be periodically renewed without changing these secrets. Meanwhile, based on the intractability of the discrete logarithm, the shadows provided by participants can be verified.

Keywords: Multi-secret sharing, proactive, secret sharing

1 Introduction

A secret sharing scheme is a technique to share a secret among a group of participants. It is mainly used to protect secret information from being lost, destroyed, or modified. In 1979, the first (t, n) threshold secret sharing schemes, based on Lagrange interpolating and liner project geometry, were proposed by Shamir [12] and Blakley [1], respectively. A secret sharing scheme contains a trusted dealer and n participants. The dealer divides the shared secret into n shadows and distributes them to these n participants through a secure channel. In the (t, n) threshold scheme, at least t honest participants can reconstruct the shared secret, but $(t-1)$ or fewer participants can obtain nothing about the secret. Therefore, even though some participants are compromised, if only the number of the compromised participants is less than t, they cannot cooperate to compute the secret.

Secret sharing schemes protect the secrecy and integrity of information by distributing the information over different locations (shadow holders). However, for long-lived and sensitive secrets, this protection may be insufficient. In many situations, such as cryptographic master keys, data files, legal documents, etc., a secret value needs to be stored for a long time. In these situations, given enough time, an adversary may compromise t servers one by one, obtain t shadows, and thus learn the shared secret. Thus, in order to protect the secrecy of the information, we need to periodically renew the shadows without changing the shared secret. To prevent such an attack, proactive secret sharing schemes are proposed. Proactive security for secret sharing was firstly suggested by Ostrovsky and Yung [10]. Herzberg et al. [5] further discussed proactive secret sharing schemes and gave a detailed proactive scheme. In their scheme, shadows can be periodically renewed (without changing the secret) in such a way that information gained by the adversary in one time period is useless for attacking the secret after the shadows are renewed. Hence, the adversary willing to learn the secret needs to break to all t locations during the same time period. Xu et al. [14] proposed a secret sharing scheme with periodic renewing shadows. In their scheme, because a trusted dealer distributes the secret information in the initialization phase and renewing phase, the amount of data communication and calculation are reduced. Zhou et al. [17] proposed in 2005 a proactive secret sharing (PSS) protocol for asynchronous systems, in which message delivery delays and processor execution speeds do not have fixed bounds. Their research extended the scope of PSS. In 2009, Ma and Ding [8] proposed a proactive verifiable linear integer secret sharing scheme. Linear integer secret sharing was firstly developed by Damgard and Thorbek [2], in which the shared secret was an integer, and each shadow was computed as an integer linear combination of the shared secret and some random integers selected by the dealer. In Ma and Ding's scheme, they introduced combinatorial structure into the proactive scheme to reduce the computational cost, meanwhile, they presented a verifiable method without a public key cryptosystem, which can prevent and detect cheating both from participants and dealers. In 2010, Schultz and Liskov [11] developed a new mobile proactive secret sharing scheme. Their scheme allows the set of participants to change.

However, in their schemes, only one secret can be shared during one secret sharing process. There are also

many papers [9, 13] that discuss proactive secret sharing. Our discussion will mainly follow the papers [5, 14].

Multi-secret sharing (MSS) schemes have been proposed by Harn [4] in 1995, in order to solve the problem that several secrets can be shared during one secret sharing process. In 2004, Yang, Chang and Hwang (YCH) [15] proposed a new MSS scheme based on Shamir's secret sharing scheme and the two-variable one-way function. Later, Li et al. [7] presented a new (t, n) threshold multi-secret sharing scheme. In 2007, Zhao et al. [16] proposed a practical verifiable multi-secret sharing scheme based on YCH and Hwang-Chang (HC) schemes [6]. The verification phase of Zhao's scheme is the same as that of HC scheme. So, a secure channel is not necessary at all. In 2008, Dehkordi and Mashhadi [3] also proposed a verifiable multi-secret sharing based on YCH, the intractability of Discrete Logarithm (DL) and RSA cryptosystem. In their scheme, there is not any need to a secure channel, and verifiable property is more efficient.

In this paper, we present a practical and efficient proactive multi-secret sharing scheme based on Xu's periodic renewing shadows secret sharing scheme. The verification phase is the same as the method introduced in [16]. In the proposed scheme, the shadows kept by participants can be updated periodically without changing these secrets. Meanwhile, multiple secrets can be shared during one secret sharing process.

To the best of our knowledge, no proactive multi-secret sharing schemes have been proposed in the literature to date. The proactive multi-secret characteristic of the proposed scheme is not available in the existing mechanisms, so the proposed scheme has the potential to work in many applications. The key features of our proposed proactive multi-secret sharing scheme are summarized below.

1) Shadows held in participants can be periodically updated without changing the shared secret;
2) The participants can shared multiple secrets during one secret sharing process;
3) Every participant can verify the validity of the shadows which he/she receives and other participants show;
4) The proposed scheme is efficiency and "$\oplus$" operation is low computing cost.

The remainder of this paper is organized as follows. In Section 2, we briefly review the multi-secret sharing scheme based on a two-variable one-way function proposed by Li et al., which is the major building block of our scheme. In the next section, we demonstrate the proposed scheme. Section 4 gives some security analysis. Finally, we presents our conclusions in Section 5.

2 Review of Li Scheme

In this section, we will review the Li scheme [7]. These schemes are based the threshold scheme proposed by Shamir [12] where the secret is embedded in an interpolating polynomial and each participant keeps a shadow associated to the interpolating polynomial.

Before presenting Li's scheme, we firstly give a definition of a two-variable one-way function $f(r, s)$ with two variables r and s. The two-variable one-way function has been used in Li's schemes.

Definition 1 [15]. Function $f(r, s)$ denotes any two-variable one-way function that maps any r and s onto a bit string $f(r, s)$ of a fixed length. The two-variable one-way function has several properties:

1) Given r and s, it is easy to compute $f(r, s)$;
2) Given s and $f(r, s)$, it is hard to compute r;
3) Having no knowledge of s, it is hard to compute $f(r, s)$ for any r;
4) Given s, it is hard to find two different values r_1 and r_2 such that $f(r_1, s) = f(r_2, s)$;
5) Given r and $f(r, s)$, it is hard to compute s;
6) Given pairs of r_i and $f(r_i, s)$, it is hard to compute $f(r_j, s)$, for $r_i \neq r_j$.

Then, we introduce a theorem that has been used in Li's scheme and will also be used in our scheme.

Theorem 1. *Given $(m+1)$ unknown variables $x_i \in GF(q)\,(i = 0, 1, ..., m)$, and m equations $x'_i = x_0 \oplus x_i\,(i = 1, 2, ..., m)$, where $GF(q)$ is a finite field. Here "$\oplus$" denotes exclusive-or bit by bit. Only the values of $x'_i\,(i = 1, 2, ..., m)$, are published. Given x_0, it is easy to find the remaining unknown symbols $x_i\,(i = 1, 2, ..., m)$; without any knowledge of x_0, it is computationally infeasible to determine the values of these unknown symbols.*

Proof. We prove Theorem 1 in two steps:

1) Given x_0, we can find $x_i\,(i = 1, 2, ..., m)$ easily by computing $x_i = x_0 \oplus x'_i$.
2) Without any knowledge of x_0, Theorem 1 is equal to solve m simultaneous equations, $x_0 \oplus x_i = x'_i\,(i = 1, 2, ..., m)$, with $(m+1)$ unknown symbols $x_i\,(i = 0, 1, ..., m)$. So, given these m equations, the values of these unknown symbols cannot be of the unknown symbols. The only thing for an adversary to do is to guess the doing it is only $1/q$ due to $x_i \in GF(q)$. If $GF(q)$ is a sufficiently large finite field, the successful probability tends to 0. So with no knowledge of x_0, it is computationally infeasible to determine the values of these unknown symbols.

□

Li's scheme can be described briefly as follows:

1) System parameters. Let $GF(q)$ denote a finite field, where q is a large prime number. All numbers are elements of $GF(q)$. The dealer randomly selects n

distinct integers $s_1, s_2, ..., s_n$, from $GF(q)$ as participants secret shadows and randomly selects n distinct integers,$u_i \in [n-t+2, q]$, for $i = 1, 2, ..., n$, as participants public identifiers. There are p secrets $k_1, k_2, ..., k_p$ to be shared among n participants. Let $f(r, s)$ be a two-variable one-way function defined above, which is used to compute pseudo shadows of participants.

2) Secret distribution. The trusted dealer performs the following steps to implement the secret distribution:

   a. Randomly choose an integer r and compute $f(r, s_i)$ for $i = 1, 2, ..., n$.

   b. Use n pairs of $(0, k_1)$ and $(u_1, f(r, s_1))$, $(u_2, f(r, s_2))$,..., $(u_n, f(r, s_n))$ to construct an nth degree polynomial $h(x) = a_0 + a_1 x + ... + a_n x^n$.

   c. Compute $z_i = h(i) \bmod q$ for $i = 1, 2, ..., n-t+1$ and $k_i' = k_1 \oplus k_i \bmod q$ where $i = 2, 3, ..., p$.

   d. Publish the values of r, z_1, z_2, ..., z_{n-t+1}, k_2', k_3', $\cdots$, k_p'.

3) Secret reconstruction. In order to reconstruct the shared secrets, at least t participants pool their pseudo shadows $f(r, s_i)$ for $i = 1', 2', ..., t'$. From these t pseudo shadows, we have t pairs of $(u_i, f(r, s_i))$ for $i = 1', 2', ..., t'$. With the knowledge of the public values $z_1, z_2, ..., z_{n-t+1}$, we can get $(n-t+1)$ pairs of (i, z_i) for $i = 1, 2, ..., n-t+1$. Therefore, there are $(n+1)$ pairs obtained altogether, by which the nth degree polynomial $h(x)$ can be uniquely determined. We use (X_i, Y_i) for $i = 1, 2, ..., n+1$ to denote these $(n+1)$ pairs, respectively. So $h(0)$ can be reconstructed through the following Lagrange interpolation polynomial:

$$h(0) = \sum_{i=1}^{n+1} Y_i \prod_{j=1, j\neq i}^{n+1} \frac{-X_j}{X_i - X_j} \bmod q.$$

We have $k_1 = h(0)$, subsequently, the remained $(p-1)$ secrets can be easily found by for $i = 2, 3, ..., p$, respectively.

3 The Proposed Scheme

In this section we will propose a new (k, n) threshold proactive multi-secret sharing scheme that are based on Xu's proactive secret sharing scheme. The sharing multiple secrets method is based on Li's multi-secret sharing scheme.

Like Li's scheme, our scheme is based on Theorem 1, and the scheme can be described as follows:

1) System parameters. The dealer (denoted as U_D) first creates a public notice board (NB), whose properties are as same as those in Type 1 scheme. We assume that $EP_i(.)$ are the public key encryption algorithm using the participants public key and the encryption process are secure and reliable. Let q be a large prime, and let $GF(q)$ denote a finite field, such that computing discrete logarithms in this field is infeasible and all the numbers are elements in the finite field $GF(q)$. Let g is the generator of the finite field $GF(q)$, $g \in GF(q)$. The dealer randomly selects n distinct integers, $u_i \in GF(q)$, for $i = 1, 2, ..., n$, as participants public identifiers. Without loss of generality, we also assume that there are n participants, $U_1, U_2, ..., U_n$, sharing p secrets $P_1, P_2, ..., P_p$, $P_1, P_2, ..., P_p \in GF(q)$.

   The notations utilized in this paper are listed in Table 1.

2) Secret distribution. The shadows computed in period t are denoted by using the superscript (t), i.e., $y_i{}^{(t)}, t = 0, 1, ...$ The polynomial corresponding to these shadows is denoted $f^{(t)}(.)$. At the beginning of the time period, the trusted dealer executes the following steps:

   a. Construct a $(k-1)$th degree polynomial $f^{(0)}(x) = a_0 + a_1^{(0)} x + \cdots + a_{k-1}^{(0)} x^{k-1} \bmod q$, where $a_0 = P_1$ and are randomly chosen from $GF(q)$.

   b. Compute $y_i^{(0)} = f^{(0)}(u_i) \bmod q, (i = 1, 2, ..., n)$, and distributes $y_i^{(0)}$ to every participants U_i for $i = 1, 2, ..., n$, over a security channel.

   c. The trusted dealer compute $G_i^{(0)} = g^{y_i^{(0)}} \bmod q$, for $i = 1, 2, ..., n$, and publish $\left\{g, G_i{}^{(0)} (i = 1, 2, ..., n)\right\}$ on the notice board.

   d. Compute $P_i' = P_1 \oplus P_i \bmod q$, for $i = 2, 3, ..., p$, and publish $\{P_i' (i = 2, 3, ..., p)\}$ on the notice board.

3) Shadow renewal. To renew the shadows at period t, $t = 1, 2, ...$, the renewed protocol will be performed as follows:

   a. Randomly select $k-1$ integers from the finite field $GF(q)$,$\varepsilon_1^{(t)}, \varepsilon_2^{(t)}, \ldots, \varepsilon_{k-1}^{(t)}$, and construct an polynomial $\varepsilon^{(t)}(x) = \varepsilon_1^{(t)} x + \varepsilon_2^{(t)} x^2 + \ldots + \varepsilon_{k-1}^{(t)} x^{k-1} \bmod q$.

   b. Compute $u_i^{(t)} = \varepsilon^{(t)}(i)$,$v_i^{(t)} = EP_i(u_i^{(t)})$,$i = 1, 2, ..., n$, and $G_i^{(t)} = g^{y_i^{(t-1)}} \cdot g^{u_i^{(t)}} \bmod q$, $(i = 1, 2, ..., n)$, and publish $\left\{v_i^{(t)}, G_i^{(t)} (i = 1, 2, ..., n)\right\}$ on the notice board.

   c. At time period t, each participant U_i will decrypt $v_i^{(t)} = EP_i(u_i^{(t)})$ using its own private key, and it will be able to obtain $u_i^{(t)}$. By the linearity of the polynomial evaluation operation, we get the renewal of the shadows $y_i^{(t)} \leftarrow y_i^{(t-1)} +$

Table 1: The notations

$u_1, u_2, ..., u_n$	participants' public identifiers
k	threshold value
$t, t = 1, 2, 3, ...$	time period
$U_1, U_2, ..., U_n$	n participants
$P_1, P_2, ..., P_p$	p shared secrets
$\varepsilon^{(t)}(x)$	the updated polynomial at t period time
$u_i^{(t)}$	the updated value at t period on ith shadow

$u_i^{(t)}$ according to $f^{(t)}(x) \leftarrow f^{(t-1)}(x) + \varepsilon^{(t)}(x)$, and destroy $y_i^{(t-1)}$.

4) Secret reconstruction. At time period t, without losing generality, suppose k participants U_i, $i = 1, 2, ..., k$, pool their shadows $y_i^{(t)*}$ (for $i = 1, 2, ..., k$), every participant U_i can check whether others secret shadows are valid by the following equations:

$$g^{y_i^{(t)*}} = G_i^{(t)} \bmod q.$$

Then, with the knowledge of k pairs $\left(u_1, y_1^{(t)}\right)$, $\left(u_2, y_2^{(t)}\right)$,..., $\left(u_k, y_k^{(t)}\right)$, the $(k-1)$th polynomial $f^{(t)}(x)$ can be uniquely determined as

$$f^{(t)}(x) = \sum_{i=1}^{k} y_i^{(t)} \prod_{j=1, j\neq i}^{k} \frac{x - u_j}{u_i - u_j}.$$

We have $P_1 = f^{(t)}(0) = a_0$, subsequently, the remained $(p-1)$ secrets can be easily found by $P_i = P_1 \oplus P_i' \bmod q$, for $i = 2, 3, ..., p$, respectively.

4 Security Analysis

In this paper, we proposed two proactive multi-secret sharing schemes based on Xu's periodic renewing shadows secret sharing scheme. The security of the proposed scheme is based on the security of Li's multi-secret sharing scheme and discrete logarithm problem. In the following, several possible attacks are investigated to demonstrate the security of the proposed scheme.

Attack 1. $(t-1)$ or fewer participants try to recover secrets.

Analysis: The security of the proposed scheme, similar to the security of Shamir's scheme is based on the Lagrange interpolation polynomial. And, any $(k-1)$ or fewer participants cannot compute the polynomial $f(x)$ and obtain anything about the secrets.

Attack 2. A malicious adversary may try to reveal k secret shadows of participants in a long time.

Analysis: According to the characteristic of proactive secret sharing and the description of the proposed scheme, the shadows kept by participants can be updated periodically. That is, the shadows will be changed at regular intervals. Therefore, a malicious adversary need to reveals k secret shadows of participants in a period time. Otherwise, if only $(k-1)$ secret shadows are revealed in a period time, and another secret shadow is revealed in the next period, the malicious adversary cannot obtain the shared secret since one secret shadow have been changed. The revealed k secret shadows cannot reconstruct the $(k-1)$th degree polynomial. The proactive characteristic of the proposed scheme increases the degree of attack difficulty.

Attack 3. A malicious participant tries to pool a fake pseudo shadow s_i' to cheat other cooperators.

Analysis: In the process of reconstructing the shared secrets, we usually assumed that the involved participants must provide their shadows honestly when they want to cooperate to recover the secrets. However, this assumption is impractical. A malicious participant can pool a fake pseudo shadow s_i' to other participants. This will lead to that other participants providing their shadows honestly cannot reconstruct the shared secrets from the $(t-1)$ corrected shadows, and only the malicious participant can obtain the secrets. In the proposed scheme, we present a verification method based on the intractability of the discrete logarithm. Every participant U_i can check whether others secret shadows $y_j^{(t)*}s$(for $j = 1, 2, ..., k, j \neq i$) are valid by the following equations:$g^{y_i^{(t)*}} = G_i^{(t)} \bmod q$.

5 Conclusions

In this paper, we present a novel proactive multi-secret sharing scheme based on Xu et al.'s scheme and the intractability of the discrete logarithm. The scheme realizes the property of proactive. That is, shadows held by every participant can be updated in a period time. As to an adversary, if he wants to attack the shared secret, he must compromise t servers one by one in one time period. How-

ever, it is difficult. Compared with the previous works, in our scheme, multiple secrets can be shared during one secret sharing process. In addition, in the reconstruction phase, the shadows can be verified.

Acknowledgments

This paper is supported by the National Science Foundation of China under grant No. 61272173, 61100194, 61401060 and the general program of Liaoning Provincial Department of Education Science Research under grants L2014017.

References

[1] G. Blakley, "Safeguarding cryptographic keys," in *In Proceedings of the National Computer Conference*, pp. 313–317, Montvale: NCC, 1979.

[2] I. Damgard and R. Thorbek, "Linear integer secret sharing and distributed exponentiation," in *In Proceedings of 9th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2006)*, pp. 75–90, New York, USA, April 2006.

[3] M.H. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Computer Standards & Interfaces*, vol. 30, no. 3, pp. 187–190, 2008.

[4] L. Harn, "Efficient sharing (broadcasting) of multiple secret," *IEE Proceedings Computers and Digital Technique*, vol. 142, no. 3, pp. 237–240, 1995.

[5] A. Herzberg, S.L. Jarecki, and H. Krawczyk et al., "Proactive secret sharing or: How to cope with perpetual leakage," in *In Advances in Cryptology-Crypto95*, pp. 339–352, Berlin: Springer-Verlag, 1995.

[6] R.J. Hwang and C.C. Chang, "An on-line secret sharing scheme for multi secrets," *Computer Communications*, vol. 21, no. 13, pp. 1170–1176, 1998.

[7] H.X. Li, C.T. Cheng, and L.J. Pang, "A new (t, n)- threshold multi-secret sharing scheme," in *In Proceedings of the 2005 International Conference on Computational Intelligence and Security (CIS 2005), Part II, LNAI 3802*, pp. 421–426, 2005.

[8] C.G. Ma and X.F. Ding, "Proactive verifiable linear integer secret sharing scheme," in *In Proceedings of 11th International Conference on Information and Communications Security (ICICS 2009)*, pp. 439–448, Beijing, China, 2009.

[9] V. Nikov, S. Nikova, B. Preneel, and J. Vandewalle, "Applying general access structure to proactive secret sharing schemes," in *In Proceedings of the 23th Symposium on Information Theory*, pp. 29–31, Benelus, 2002.

[10] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks," in *In Proceeding of 10th the ACM Symposium on Principles of Distributed Computing (PODC'91)*, pp. 51–59, New York, USA, 1979.

[11] D. Schultz and B. Liskov, "Mpss: Mobile proactive secret sharing," *ACM Transactions on Information and System Security*, vol. 13, no. 4, pp. 34–65, 2010.

[12] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[13] D.R. Stinson and R. Wei, "Unconditionally secure proactive secret sharing scheme with combinatorial structure," in *In Proceedings of the 6th International Workshop on Selected Areas in Cryptography (SAC99)), Springer-Verlag, LNCS 1758*, pp. 200–214, London, UK, 1999.

[14] C.X. Xu, S.M., and G.Z. Xiao, "A secret sharing scheme with periodic renewing to identify cheaters," *Chinese Journal of Computers*, vol. 25, no. 6, pp. 657–660, 2002.

[15] C.C. Yang, T.Y. Chang, and M.S. Hwang, "A (t, n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.

[16] J.J Zhao, J.Z. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 138–141, 2007.

[17] L.D. Zou, F.B. Schneider, and R.V. Renesse, "Apss: Proactive secret sharing in asynchronous systems," *ACM Transaction on Information and System Security*, vol. 8, no. 3, pp. 259–286, 2005.

Bin Feng received the BS degree in Computer Science and Technology in 2002 from the LiaoCheng University, Shandong, China, and the MS degree in software engineering in 2006 from the Dalian University of Technology, Dalian, China. He has been an assistant in TaiShan College among 2002-2004. He is currently a full engineer of Computer Science at DaLian University of Technology (DLUT) (Dalian, China), where he has been since September 2006. Since 2011 he is currently pursuing his PhD degree in computer software and theory from the Dalian University of Technology, Dalian, China. His research interests include data hiding, image processing, network and information security.

Cheng Guo received the B.S. degree in computer science from Xi'an University of Architecture and Technology in 2002. He received the M.S. degree in 2006 and his Ph.D in computer application and technology, in 2009, both from the Dalian University of Technology, Dalian, China. From July 2010 to July 2012, he was a post doc in the Department of Computer Science at the National Tsing Hua University, Hsinchu, Taiwan. Since 2013, he has been an associate professor in the School of Software Technology at the Dalian University of Technology. His current research interests include information security and cryptology.

Mingchu Li received the B.S. degree in mathematics, Jiangxi Normal University and the M.S. degree in applied science , University of Science and Technology Beijing in 1983 and 1989, respectively. He worked for University of Science and Technology Beijing in the capacity of

associate professor from 1989 to 1994. He received his doctorate in Mathematics, University of Toronto in 1997. He was engaged in research and development on information security at Longview Solution Inc, Compuware Inc. from 1997 to 2002. From 2002, he worked for School of Software of Tianjin University as a full professor, and from 2004 to now, he worked for School of Software Technology of Dalian University of Technology as a full Professor, Ph.D. supervisor, and vice dean. His main research interests include theoretical computer science and cryptography.

Zhi-Hui Wang was born in Inner Mongolia in 1982. She received her B.S. degree in software engineering from the North Eastern University, Shenyang in 2004, M.S. degree in software engineering from Dalian University of Technology (DUT), Dalian in 2007, and Ph.D. degree in computer software and theory from DUT in 2010. Since 2014, she has been an associated professor in the School of Software Technology at the Dalian University of Technology. Her current research interests include information hiding and image processing.