VDGMSISS: A Verifiable and Detectable Multi-Secret Images Sharing Scheme with General Access Structure

Justie Su-Tzu Juan, Ming-Jheng Li, Ching-Fen Lee, Ruei-Yu Wu

Abstract—A secret image sharing scheme is a way to protect images. The main idea is dispersing the secret image into numerous shadow images. A secret image sharing scheme can withstand the impersonal attack and achieve the highly practical property of multi-use is more practical. Therefore, this paper proposes a verifiable and detectable secret image-sharing scheme called VDGMSISS to solve the impersonal attack and to achieve some properties such as encrypting multi-secret images at one time and multi-use. Moreover, our scheme can also be used for any general access structure.

Keywords—Multi-secret images sharing scheme, verifiable, detectable, general access structure.

I. Introduction

With the fast development of information science and technology, the Internet becomes part of modern life progressively. Over the Internet, many digital materials such as military documents, important images, and communications regarding commercial affairs can be accessed conveniently by various users. Hence, security has become significant issue. To address the aforementioned problems, many image protection techniques have been proposed, including visual and polynomial approaches. Thus far, visual cryptography approaches have been popular. Visual cryptography can be extended with secret sharing concepts. Visual cryptography was proposed by Naor and Shamir [6] in 1995. Regarding polynomial approaches, secret sharing schemes (SSSs) have been independently introduced by Blakley [1] and Shamir [8]. The typical SSS is a method for distributing a secret among several participants, each of which is allocated a share of the secret, in such a way that only qualified subsets of the participants can reconstruct it and unqualified subsets receive no information about the secret.

In visual cryptography, the secret image is distributed in many shared transparencies, each of which consists of many noisy black dots. After the secret image has been distributed, it can be recovered by superimposing any t shared without any equipment and cryptographic protocol. However, two defects of visual cryptography are that (1) the recovered image is lossy and (2) pixel expansion impairs quality. Consequently, Thien and Lin [10] proposed a secret image sharing method derived from the (t, n)-threshold scheme in 2002. In [10], the size of each shared image is smaller than that of the secret image and the recovered image is lossless. Wang et al. [11] and Zhao et al. [12] then proposed secret image sharing schemes based on [10]. Nevertheless, these schemes are only suitable for a single grayscale image. In addition, [10], [11] does not offer verification. Hence, Zhao et al. [12] presented a verifiable image secret sharing scheme based on [10] and the discrete logarithm problem in 2009 and claim that their scheme can achieve the property of verification. But their scheme is not guaranteed to detect whether the dealer is a cheater. Moreover, their scheme neither applies to colored images nor shares multi-secret and multi-use images at the same time. In addition, their scheme does not realize general access structure as discussed in [5].

Theoretically, the *access structure* $\Gamma \subseteq 2^P$ is the set of all qualified subsets. For any qualified subset $A \in \Gamma$, any superset of A is also a qualified subset. Hence, the access structure should satisfy the *monotone increasing property*: If $A \in \Gamma$ and $A \subseteq B \subseteq P$, $B \in \Gamma$. Let Γ' be a family of the minimal sets in Γ, called the *minimal access structure*. That is, $\Gamma' = \{A \in \Gamma : A' \not\subset A \text{ for all } A' \in \Gamma - \{A\}\}$. We only consider Γ' in the proposed scheme. In a multi-secret images sharing scheme, the dealer distributes z secret images I_1, I_2, …, I_z with their associated access structures Γ'_1, Γ'_2, …, Γ'_z.

A. Contributions

In this paper, we present a verifiable and detectable multi-secret images sharing scheme with general access structure, which can improve on the scheme of Zhao et al. [12]. The scheme offers six contributions:

1) The proposed scheme (called VDGMSISS) can identify any cheater.
2) VDGMSISS does not require any existing secret channel between the dealer and the participants.
3) All the sizes of the shared images are less than those of the lossless method of Zhao et al. when each segment has d_i pixels for $1 \leq i \leq z$.
4) VDGMSISS can share multi-secret images and can be multi-use at the same time.
5) VDGMSISS can share both grayscale and colored images.
6) VDGMSISS can realize general access structure.

The remainder of this paper is organized as follows. In Section II, we briefly review the Schnorr digital signature scheme and the scheme of Zhao et al. Section III presents

Justie Su-Tzu Juan, Ming-Jheng Li, and Ching-Fen Lee are with the Department of Computer Science and Information Engineering National Chi Nan University Puli, Nantou 54561, Taiwan (e-mail: jsjuan@ncnu.edu.tw).

Ruei-Yu Wu is with Department of Management Information Systems, Hwa Hsia University of Technology, Taiwan.

the proposed scheme in detail. Next, the experimental results and some analysis of the proposed scheme are demonstrated in Sections IV and V. Finally, the current conclusion is provided in Section VI.

II. Related Works

A. Schnorr Digital Signature Scheme

In 1985, Schnorr [9] proposed a digital signature scheme based on discrete logarithm problem. It is considered the simplest digital signature scheme. The detailed scheme is described as follows.

Setup of System Parameters

1) A signer (or a system) first selects two large primes p and q such that $q|p-1$, where $q \geq 2^{160}$ and $p \geq 2^{512}$.
2) Choose $g \in Z_p$, such that $g^q = 1 \bmod p$.
3) Let $h(.)$ be an two-variables one-way hash function over Z_q.

Setup of A Principal's Public/ Private Key

A signer chooses a random number $x \in_R Z_q^*$, and then computes $y = g^x \bmod p$, where (x, y) is signer's private/public keys pair.

Signature Generation

Input the message m to create a signature.

1) The signer chooses a random number $k \in Z_q^*$ and then computes $r = g^k \bmod p$.
2) Compute $e = h(r, m) \bmod q$.
3) Evaluate $s = k - xe \bmod q$.

Return (e, s), which is the signature of the message m.

Signature Verification

To verify that whether (e, s) is a valid signature of message m, verifier can do the following steps:

1) $r' = g^s y^e \bmod p$.
2) Check that whether the equation $e = h(r', m) \bmod q$ holds. If it holds, (e, s) is a valid signature of the message m.

B. Review of the Scheme of Zhao et al. [12]

In this subsection, we only review the lossless method of Zhao et al. [12]. This method can divide a secret grayscale image I into n publicly shared images; each participant holds a secret share. By using subsecrets of any more than t (or equal to t) participants and the corresponding public shared images, any qualified subset can reconstruct I as a lossless image, where size of I is $w \times h$ and each generated shared image is approximately $1/t$ the size of I. Let the prime number p be 251. To apply this method, they slightly modify their lossy method to realize the lossless version. This algorithm can be divided into three phases: initialization, distribution, and reconstruction with verification.

Initialization Phase:

The dealer D and each participants P_i can use the following steps to intercommunicate over a public channel for $1 \leq i \leq n$.

1. D chooses two prime numbers p, q, and computes $S = pq$, where p and q should satisfy the same properties as the two primes used in RSA cryptosystem [7].
2. D chooses an integer $g \in [S^{1/2}, S]$, such that g is relatively prime to p and q and publishes $\{g, S\}$ on notice board (*NB*).
3. P_i randomly selects $s_i \in_R [2, S]$ as own secret share and computes $R_i = g^{s_i} \bmod S$ for $1 \leq i \leq n$.
4. P_i provides R_i to D. And then, D must ensure that $R_i \neq R_m$ and publishes R_i for all $P_i \neq P_m$. Once R_i is equal to R_m for some participant P_m, D should demand P_i to choose new s_i.

Distribution Phase:

D can use the following steps to share the secret grayscale image I among n participants.

1. D sequentially reads gray values v_k of I for $1 \leq k \leq |E|$ and then stores in the array E according to the following rules:
   (a). If $v_k < 250$, D stores v_k in the array E.
   (b). If $v_k \geq 250$, D stores 250 and $(v_k - 250)$ in E.
2. D randomly chooses an integer $s_0 \in_R [2, S]$, and lets gcd($s_0, p-1$) = gcd($s_0, q-1$) = 1. After, D computes f, such that $s_0 \times f = 1 \bmod \phi(S)$, where $\phi(S)$ is Euler's totient function.
3. D computes $R_0 = g^{s_0} \bmod S$ and sub-secret $U_i = R_i^{s_0} \bmod S$ and publishes $\{R_0, f\}$ on *NB* for $1 \leq i \leq n$.
4. D sequentially takes t not-shared-yet elements of E to set up a segment.
5. D uses the segment of above step and constructs $t-1$ degree polynomial $b_j(x)$ of degree $t-1$ as follows:
$$b_j(x) = a_{j,0} + a_{j,1}x + \ldots + a_{j,t-1}x^{t-1} \bmod 251,$$
where $a_{j,0}, \ldots, a_{j,t-1}$ are the t pixels of the segment j for $1 \leq j \leq |E|/t$.
6. D computes $y_{j,i} = b_j(U_i)$ for $1 \leq i \leq n$, $1 \leq j \leq |E|/t$.
7. D repeats Steps 4–6 until all elements of E are processed.
8. D merges $y_{j,i}$ into a public image Y_i from all shared value $y_{j,i}$ and publishes Y_i on *NB* for $1 \leq i \leq n$, $1 \leq j \leq |E|/t$.

Reconstruction and Verification Phases:

When the anyone (Combiner C) of more than (or equal to) t participants get together, they can reconstruct the secret grayscale image I with lossless by using their sub-secrets and the corresponding public shared images.

1. Each of more than (or equal to) t participants computes own sub-secret $U_i' = R_0^{s_i} \bmod S$, where s_i is a secret share of P_i for $1 \leq i \leq n$.
2. Anyone can verify U_i' that provided by P_i for $1 \leq i \leq n$:
$$\begin{cases} \text{true}, & \text{if } U_i'^{f} = R_i \bmod S; \\ \text{false}, & \text{otherwise}. \end{cases}$$
If the result of the verification is false, the participant P_i may be a cheater.
3. C uses any t pairs of $(U_i', b_j(U_i'))$ and the Lagrange's interpolation formula to reconstruct the coefficients $a_{j,0}$, …, $a_{j,t-1}$ for $1 \leq i \leq n$, $1 \leq j \leq |E|/t$.

4. The coefficients $a_{j,0}$, ..., $a_{j,t-1}$ in the above step are the corresponding t elements of the segment j of E for $1 \leq j \leq |E|/t$.
5. C sequentially reads the elements $\{v_k\}$ of E and stores in I with lossless according to the following rules for $1 \leq k \leq |E|$.
   (a). If $v_k < 250$, D stores v_k in I and deletes v_k from E.
   (a). If $v_k = 250$, D reads v_{k+1} immediately, then stores $(250 + v_{k+1})$ in I and deletes v_k, v_{k+1} from E.

C. Analysis of the Scheme of Zhao et al. [12]

In this subsection, we argue that the scheme of Zhao et al. is not secure and efficient enough in some situations.

1) Impersonal Attack: Because the dealer D has the value $U_i = U'_i$ for any i, if a adversary A attacks D and obtains U_i for some participant P_i, or D is not trusted enough, then A or D may impersonate a valid participant P_i to participate in reconstruction, and then take the secret image I to do illegal things, such as copyright piracy, to cause P_i be punished or fined.

2) The Multi-use Property: Aside from $U'_{i_1}, U'_{i_2}, \ldots, U'_{i_t}$, if this scheme does not change any participant, then this scheme cannot provide multi-use because the sub-secrets have been known by the participants in the first sharing session, then in the next sharing session the secret image can be reconstructed without collecting sub-secrets. This problem can be avoided with a new image I and the distribution of public images Y_i for $1 \leq i \leq n$.

To address the aforementioned problems, we proposed a verifiable and detectable secret image sharing scheme. The proposed scheme can share multiple secret images and realize general access structure.

III. The Proposed Scheme: VDGMSISS

In this section, our verifiable and detectable secret image-sharing scheme with general access structure is proposed. Subsection III *A* presents the parameter configuration. In Subsections III *B-D*, we introduce initialization, distribution, and reconstruction with verification of the proposed scheme.

A. Parameter Setup

Let $P = \{P_1, P_2, \ldots, P_n\}$ be the set of these n participant and $Q = \{I_1, I_2, \ldots, I_z\}$ be the set of the z images, where the size of I_j is $w_j \times h_j$ for $1 \leq j \leq z$. Note that the size of these z secret images may be different. Let $\Gamma'_j = \{A_{j,1}, A_{j,2}, \ldots, A_{j,|\Gamma'_j|}\}$ is the minimal access structure of each secret image I_j for $1 \leq j \leq z$. We assume that the participants in $A_{j,u} = \{P_{j,u,1}, P_{j,u,2}, \ldots, P_{j,u,|A_{j,u}|}\}$ for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$. Without loss of generality, assume that there is a dealer D and the notice board *NB* which is required for D to publish public information. Let $h(r, s)$ be a two-variables one-way hash function over Z_q with two input parameters r and s, $H(.)$ be an one-way hash function over Z_q and "$\oplus$" be the *exclusive-or* operation. The computations of all polynomials are in finite field GF(2^8). Let irreducible polynomial of degree 8 be $m(x) = x^8 + x^4 + x^3 + x^2 + 1$. All public information should be published on *NB*.

B. Initialization Phase

D and each participant chooses their own secret share, separately. Moreover, D also setups system parameters and qualified subsets. Then, D and each participant selects their own secret session number.

1. D randomly chooses two distinct nonzero elements g, q from GF(p), where p and q are two large prime numbers with $q|p-1$ and $g^q = 1 \mod p$. And then D publishes g, q and p on *NB*.
2. D randomly chooses an integer x_0 from GF(p) as a secret share for itself and computes $R_0 = g^{x_0} \mod p$.
3. Each participant randomly chooses an integer x_i from GF(p) as a secret share for itself, computes $R_i = g^{x_i} \mod p$ and provides R_i to D for $1 \leq i \leq n$.
4. D must check that whether $R_i \neq R_k$ for all participants $P_i \neq P_k$. Once $R_i = R_k$, D should demand participant P_i to choose new x_i. Otherwise, D publishes R_0 and R_i on *NB* for $1 \leq i \leq n$.
5. The participants in $A_{j,u}$ agree on a secret session number $b_{j,u}$ in advance, then use it to compute $R_{j,u} = g^{b_{j,u}} \mod p$ and provide $R_{j,u}$ to D for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$.
6. D must check that whether $R_{j,u} \neq R_{j',u'}$ for all $A_{j,u} \neq A_{j',u'}$. Once $R_{j,u}$ is equal to $R_{j',u'}$, D should demand the participants in $A_{j,u}$ to choose new $b_{j,u}$. Otherwise, D publishes $R_{j,u}$ on *NB* for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$.

C. Distribution Phase

The following steps are for D to process each secret image I_j among each qualified set $A_{j,u} \in \Gamma'_j$ for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$.

1. D uses a *seed* to generate a permutation sequence to permute the pixels of the secret images I_j to I'_j for $1 \leq j \leq z$.
2. D selects z suitable numbers d_j and constructs the $(d_j - 1)$ degree polynomial $f_j^\alpha(x)$ from I'_j divided into the segments, each of which has d_j pixels, for $1 \leq j \leq z$ as follows (over $GF(2^8)$):
$$f_j^\alpha(x) = \textstyle\sum_{\beta=1}^{d_j} c_j^{\alpha,\beta} x^{d_j-\beta} \text{ mod } m(x).$$
where the $c_j^{\alpha,\beta}$ is the β^{th} pixel in α^{th} segment for $1 \leq j \leq z$, $1 \leq \alpha \leq l_j = (w_j \times h_j)/d_j$ and $1 \leq \beta \leq d_j$.
3. D computes $U_{j,u} = R_{j,u}^{x_0} \mod p$ and $v_{j,u} = h(U_{j,u}, a)$ and the public random number $a \in_R Z_p^*$ and random *seed* are published on *NB* for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$.
4. D computes $V_{j,u} = v_{j,u} \oplus (\bigoplus_{P_i \in A_{j,u}} h(R_i^{x_0}, v_{j,u}))$, $H_{j,u} = H(h(R_i^{x_0}, v_{j,u}))$ and publishes $H_{j,u}$ on *NB* for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$.
5. Each participant $P_i \in A_{j,u}$ computes and checks whether $H(h(R_0^{x_i}, v'_{j,u})) = H_{j,u}$. Where $v'_{j,u} = h(R_0^{b_{j,u}} \mod p$, a). If it holds, D is honest; otherwise, participants must complain to D.
6. D computes $y_{\alpha,j,u} = f_j^\alpha(V_{j,u})$, merges it into the shared image $Y_{j,u}$ and publishes $Y_{j,u}$ on *NB* for $1 \leq \alpha \leq l_j$, $1 \leq j \leq z$ and $1 \leq u \leq |\Gamma'_j|$.
7. For $1 \leq \alpha \leq l_j$ and $1 \leq j \leq z$, D publishes additional $d_j - 1$ pairs $(V_y^j, f_j^\alpha(V_y^j))$ on *NB*, where $V_y^j \neq V_{j,u}$ for all $1 \leq y \leq d_j - 1$.

D. Reconstruction and Verification Phases

The following steps are for anyone (combiner C) of these participants in $A_{j,u}$ obtains sub-secret unique identification $V'_{j,u}$ of a qualified subset $A_{j,u}$ and finds the corresponding shared image $Y_{j,u}$ on *NB* and uses other $d_j - 1$ pairs (V^j_y, $f^\alpha_j(V^j_y)$) on *NB* to reconstruct the I_j secret images.

1. C computes $U'_{j,u} = R_0^{b_{j,u}} \bmod p$ and $v'_{j,u} = h(U'_{j,u}, a)$, where $b_{j,u}$ is the secret session number of agreement of $A_{j,u}$ in advance and a is public information on *NB* for 1 $\leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$.
2. C receives $h(R_0^{x_i}, v'_{j,u})$ and signature ($h(R_0^{x_i}, v'_{j,u})$, e_i, s_i) computed by each participant $P_i \in A_{j,u}$ for $1 \leq j \leq z$, 1 $\leq u \leq |\Gamma'_j|$, $1 \leq i \leq n$. The signature (e_i, s_i) is computed as follows:
   (a). P_i computes $r_i = g^{k_i} \bmod p$, where k_i is chosen by P_i.
   (b). P_i computes $e_i = h(r_i, h(R_0^{x_i}, v'_{j,u})) \bmod q$.
   (c). P_i computes $s_i = k_i - x_i e_i \bmod q$.
3. C verifies the signature ($h(R_0^{x_i}, v'_{j,u})$, e_i, s_i) provided by P_i and detects validity of message $h(R_0^{x_i}, v'_{j,u})$:
   (a). Verification: C computes $r'_i = g^{s_i} R_i^{e_i} \bmod p$

   $$\begin{cases} \text{true}, & \text{if } e_i \equiv h(r'_i, h(R_0^{x_i}, v'_{j,u})) \pmod{q}; \\ \text{false}, & \text{otherwise.} \end{cases}$$

   If the result of the verification is true, the message $h(R_0^{x_i}, v'_{j,u})$ is provided by P_i, obviously.

   (b). Detection: C computes $H(h(R_0^{x_i}, v'_{j,u}))$ and compares it with $H_{j,u} = H(h(R_i^{x_0}, v_{i,u}))$ on *NB*:

   $$\begin{cases} \text{true}, & \text{if } H(h(R_0^{x_i}, v'_{j,u})) = H(h(R_i^{x_0}, v_{j,u})); \\ \text{false}, & \text{otherwise.} \end{cases}$$

   If the result of the detection is true, the message $h(R_0^{x_i}, v'_{j,u})$ is correct.
4. C computes $V'_{j,u}$ = $v'_{j,u} \oplus (\bigoplus_{P_t \in A_{j,u}} h(R_0^{x_t}, v'_{j,u}))$ for 1 $\leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$, $1 \leq t \leq n$.
5. C uses $(V'_{j,u}, Y_{j,u})$ and other $d_j - 1$ pairs (V^j_y, $f^\alpha_j(V^j_y)$) on *NB* to reconstruct permuted image with the Lagrange's interpolation formula and uses the same *seed* to apply the inverse-permutation operation to the permuted image to obtain I_j for $1 \leq j \leq z$, $1 \leq u \leq |\Gamma'_j|$. Note that $Y_{j,u}$ is also published on *NB*.
6. C checks the reconstructed image. If the reconstructed image is meaningless, D is a cheater; otherwise D is honest.

IV. Experimental Results

The following are our experimental results by implementing VDGMSISS. The experimental results are conducted on a NoteBook with an Intel Core 2 CPU 2GHz and 2GB RAM. The operating system is Windows Vista, and VDGMSISS is programmed by MATLAB.

In this experiment, let D be the dealer, $P = \{P_1, P_2, P_3\}$ be the set of participants, $Z = \{I_1, I_2\}$ be the set of two secret images, where I_1 is 512 × 512 "*Jet*" and I_2 is 256 × 192 "*NCNU*," as shown in Fig. 1, and Γ'_1 and Γ'_2 be the minimal access structures of two secret images I_1 and I_2, respectively, where $\Gamma'_1 = \{A_{1,1}, A_{1,2}\}$ and $\Gamma'_2 = \{A_{2,1}\}$, where $A_{1,1} = \{P_1, P_2\}$, $A_{1,2} = \{P_2, P_3\}$, and $A_{2,1} = \{P_1, P_3\}$.

(a) *Jet* (I_1) (b) *NCNU* (I_2)

Fig. 1 Secret images for VDGMSISS

Let $d_1 = 2$ and $d_2 = 4$. Fig. 2 shows shared images $Y_{1,1}$, $Y_{1,2}$, $Y_{2,1}$ published on *NB* for $A_{1,1}$, $A_{1,2}$, $A_{2,1}$, respectively. Fig. 3 shows published public $d_1 - 1$ public pairs and $d_2 - 1$ public pairs for Γ'_1 and Γ'_2. In the reconstruction and verification phases of the proposed scheme, qualified subsets $A_{1,1}$, $A_{1,2}$, $A_{2,1}$ can reconstruct secret images I_1, I_1, I_2, respectively, as shown in Fig. 4.

V. Performance and Security Analysis

In this section, we analyze three aspects of the performance and security of VDGMSISS. First, we offer a feasibility analysis in Subsection V A. A security analysis is offered in Subsection V B. Finally, capability analysis is presented in the last subsection.

A. Feasibility Analysis

Three results published by Shamir [8], Schnorr [9], and Harn [4] guarantee the feasibility of the Lagrange interpolation polynomial, of digital signature verification and one-way hash function, and of the two-variable one-way hash function, respectively. We only analyze the feasibility of sub-secrets $V'_{j,u}$ in the proposed scheme.

Theorem 1: The sub-secret $V'_{j,u}$ is provided by the qualified subset $A_{j,u}$ iff the qualified subset $A_{j,u}$ can reconstruct secret image I_j for all $1 \leq j \leq z$ and $1 \leq u \leq |\Gamma'_j|$.

Proof: Because *NB* has $d_j - 1$ public images, $d_j - 1$ identifications V^j_y and one shared image, which consists of $f^\alpha_j(V_{j,u})$ for $1 \leq \alpha \leq l_j$, we only prove $V'_{j,u} = V_{j,u}$ then C can reconstruct secret image I_j, where $V'_{j,u}$ = $v'_{j,u}$ $\oplus$ $(\bigoplus_{P_i \in A_{j,u}} h(R_0^{x_i}, v'_{j,u}))$ and $v'_{j,u} = h(R_0^{b_{j,u}},\ a) \bmod q$; $V_{j,u}$ = $v_{j,u} \oplus (\bigoplus_{P_i \in A_{j,u}} h(R_i^{x_0}, v_{j,u}))$ and $v_{j,u} = h(R_{j,u}^{x_0},\ a)$ mod q. By the proposed scheme, $R_0^{x_i}$ = $g^{x_0 x_i} = g^{x_i x_0} = R_i^{x_0}$ mod p and $R_0^{b_{j,u}}$ = $g^{x_0 b_{j,u}} = g^{b_{j,u} x_0} = R_{j,u}^{x_0}$ mod p. Based on group are power associative, it is clearly that $R_0^{x_i} = R_i^{x_0}$ and $R_0^{b_{j,u}} = R_{j,u}^{x_0}$ over Z_p are true which implies $V'_{j,u} = V_{j,u}$ is true for all $1 \leq j \leq z$ and $1 \leq u \leq |\Gamma'_j|$. Hence, $A_{j,u}$ provides $V'_{j,u}$ can reconstruct the secret image I_j. On the opposite side, if combiner C can reconstruct the secret image I_j, then $V_{j,u}$ = $V'_{j,u}$, where $V'_{j,u}$ consists of $h(R_0^{x_i}, v'_{j,u})$ for

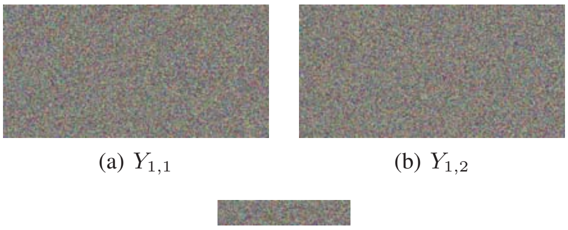
(a) $Y_{1,1}$ (b) $Y_{1,2}$ (c) $Y_{2,1}$

Fig. 2 Shared images published on *NB* for VDGMSISS

(a) public pair for Γ'_1 (b) public pair for Γ'_2 (c) public pair for Γ'_2 (d) public pair for Γ'_2

Fig. 3 Public pairs for VDGMSISS.

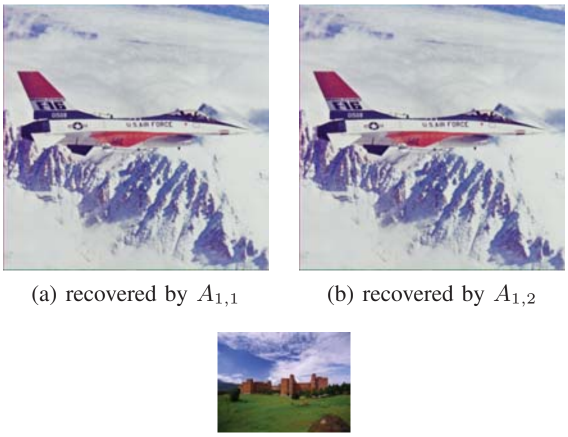
(a) recovered by $A_{1,1}$ (b) recovered by $A_{1,2}$ (c) recovered by $A_{2,1}$

Fig. 4 (a),(b), and (c) are reconstructed images

each $P_i \in A_{j,u}$. According to the property of two-variables one-way hash function, if $h(\gamma, \delta) = h(\lambda, \mu)$, $\gamma = \lambda$ and $\delta = \mu$, we have $R_0^{b_{j,u}} = R_{j,u}^{x_0}$ and $R_0^{x_i} = R_i^{x_0}$ over Z_p. By the proposed scheme, $h(R_0^{x_i}, v'_{j,u})$ carries signature (e_i, s_i), and s_i must be computed by knowing x_i. Because x_i is keeping by P_i himself, $V'_{j,u}$ must be provided by $A_{j,u}$. ■

B. Security Analysis

Because the proposed scheme uses the Lagrange interpolation formula to reconstruct sharing polynomials, the security of the proposed scheme is based on the complexity of the sharing polynomial. A polynomial function of degree $d-1$ requires at least d values to be reconstructed. We calculate the polynomial function over GF(2^8). If we only have $d-1$ equations and want to solve d unknown coefficients, the system has 2^8 possible solutions. Hence, the possibility of guessing the correct solution is $1/2^8$. In the proposed scheme, at least d shared images are required to reconstruct all sharing polynomials with the Lagrange interpolation formula. If a malicious attacker has $d-1$ shared images and wants to reconstruct all sharing polynomials, the attacker has a $(1/2^8)^l$ probability of reconstructing all sharing polynomials, where l is the number of polynomials for a secret image. For instance, if the secret image is 512×512 pixels and $d = 2$, the system has 131072 polynomials. In this case, the probability of reconstructing the secret image is $(1/2^8)^{131072}$.

In addition, if an adversary wants to derive the secret share x_i or the secret session number $b_{j,u}$ of the qualified subset $A_{j,u}$ from the public values R_i or $R_{j,u}$ on *NB*, they must solve the discrete logarithm problem [3]. However, the discrete logarithm problem is NP-intractable, and thus, the security of the proposed scheme is based on the intractability of the discrete logarithm problem.

C. Capability Analysis

This subsection compares our proposed scheme with that of Thien et al. [10] and Zhao et al. [12]. Here, we use the lossless version methods as comparative objects in the schemes of Thien et al. and Zhao et al. These comparisons require some conditions, such as the constraint that the pixels of secret images be greater than 251 and the constraint that each segment have d pixels. Next, we discuss some significant properties in detail for the proposed scheme and illustrate the notable problems of some properties in the scheme of Zhao et al.

A secret share is generated by the user in both the scheme of Zhao et al. and the proposed scheme; this is generated without existing secret communication between dealer and any participant. Therefore, no secret channel is required either in the scheme of Zhao et al. or in our proposed scheme.

In our proposed scheme, each participant $P_i \in A_{j,u}$ can use the verification procedure of the Schnorr scheme to verify the signature $(h(R_0^{x_i}, v'_{j,u}),\ e_i,\ s_i)$ of each participant P_i in $A_{j,u}$ to decide whether signature $(h(R_0^{x_i}, v'_{j,u}),\ e_i,\ s_i)$ is provided by P_i. Accordingly, our scheme can ensure that the dealer cannot impersonate participant P_i. A verifier can then detect the correctness of the messages $h(R_0^{x_i}, v'_{j,u})$ provided by P_i by computing $H(h(R_0^{x_i}, v'_{j,u}))$ and comparing it with $H(h(R_i^{x_0}, v_{j,u}))$ on *NB*. Hence, the proposed scheme is a verifiable and detectible scheme. However, in the scheme of Zhao et al., the dealer holding $U_i = R_i^{s_0} \bmod S$ can impersonate participant P_i holding $U'_i = R_0^{s_i} \bmod S$.

Zhao et al. reported that their scheme is multi-use; however, we found that if they run two sharing sessions but they do not refresh their prime numbers p, q, and g in the second sharing session, the sub-secret U'_i of each participant P_i is the same as that of the first sharing session. So, some participants know sub-secret U'_i without participant P_i providing U'_i, and fewer than t participants can use t sub-secrets to reconstruct secret image in the next sharing session. For this reason, their scheme does not satisfy the property of multi-use. But if they refresh p,

TABLE I
COMPARISONS OF VDGMSISS WITH RELATED WORKS

Capability	**[10]**	**[12]**	**Our**
Non-secret channel	No	Yes	Yes
Verification & Detection	No	No	Yes
Share colored image	No	No	Yes
Multi-secret images	No	No	Yes
Multi-use	No	No	Yes
General access structure	No	No	Yes
Size of the shared image	$\geq \frac{w \times h}{d}$	$\geq \frac{w \times h}{d}$	$= \frac{w \times h}{d}$

q, and g, the choice of p and q is limited. Because we use the two-variable one-way hash function to enable changes to the sub-secret $V'_{j,u}$ of the qualified subset $A_{j,u}$ in any later session, if two sharing sessions are executed in our proposed scheme, sub-secret $V'_{j,u}$ of each qualified subset $A_{j,u}$ in the second sharing session is in contrast to that of the first sharing session, regardless of whether we change the p, q, and g. Moreover, each participant $P_i \in A_{j,u}$ can select a secret share, keep that secret share, and reuse that secret share in the next sharing session. Thus, the proposed scheme satisfies the requirements of the multi-use property.

For each segment (d pixels of the secret image), each shared image receives one generated pixel; thus, the size of each shared image is $1/d$ of the size of the secret image. In the case where all pixels of the secret image are greater than 250, with the scheme of Zhao et al., the size of array E is double the size of the secret image. When $d = 2$, the size of each shared image is $1/2$ of the size of array E. In other words, the size of each shared image is the same as the size of the secret image in the scheme of Zhao et al. Nevertheless, in the proposed scheme, the size of each shared image always be $1/d$ of the size of the secret image for any secret image.

Finally, we summarize some comparisons between the scheme of Thien et al. [10], the scheme of Zhao et al. [12] and the proposed scheme in Table I.

VI. CONCLUSION

In this paper, we proposed a verifiable and detectable multi-secret images sharing scheme with general access structure, namely VDGMSISS. The proposed scheme solves the cheating problem in the scheme of Thien et al. and the impersonal attack problem in the scheme of Zhao et al. and delivers multi-use of secrets over time. Because all participants and the dealer choose their own secret shares, no secret communication is required between the dealer and any participant. Therefore, VDGMSISS does not need a secret channel. The proposed scheme can distribute multiple secret images, which are can be grayscale or colored images. Notably, the sizes of the shared images are smaller than those from the lossless method of [10], [12], given that secret images have more than 250 pixels and the recovered images are lossless. Furthermore, the proposed scheme realizes general access structure. Therefore, VDGMSISS is more practical and secure than schemes presented in some previous works.

ACKNOWLEDGMENT

This research was supported in part by the National Science Council of the Republic of China under grant NSC-98-2221-E-260-013- and MOST-108-2221-E-260-008-.

REFERENCES

[1] G. R. Blakley, "Safeguarding Cryptographic Keys," *Proceeding of AFIPs 1979 National Computer Conference*, Vol. 48, pp. 313-317, 1979.

[2] W. Diffie and M. Hellman "New Directions in Cryptography," *IEEE Transactions on information Theory*, Vol. 22, No. 6, pp. 644-654, 1976

[3] M. Garey and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Company, 1979.

[4] L. Harn, "Efficient Sharing (Broadcasting) of Multiple Secrets," *IEEE Proceedings-Computers and Digital Techniques*, Vol. 142, No. 3, pp. 237-240, May, 1995.

[5] M. Ito, A. Saito and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," *Proceedings of the IEEE Global Telecommunications Conference, Globecom'87*, pp. 99-102, 1987.

[6] M. Naor and A. Shamir, "Visual Cryptography," *Proceedings of Advances in Cryptology: Eurocrypt'94, Lecture Notes in Computer Science*, Vol. 950, pp. 1-12, 1995.

[7] R. L. Rivest, A. Shamir and L. Adleman "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[8] A. Shamir, "How to Share a Secret," *Communications of the ACM*, Vol. 22, No. 11, pp. 616-613, 1979.

[9] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," *Journal of Cryptology*, Vol. 4, No. 3, pp. 239-252, 1991.

[10] C. C. Thien and J. C. Lin, "Secret Image Sharing," *Computers and Graphics*, Vol. 26, No. 5, pp. 765-770, 2002.

[11] R. Z. Wang and C. H. Su, "Secret Image Sharing with Smaller Shadow Images," *Pattern Recognition Letters*, Vol. 27, No. 6, pp. 551-555, 2006.

[12] R. Zhao, J. Zhao, F. Dai and F. Zhao, "A New Image Secret Sharing Scheme to Identify Cheaters," *Computer Standards and Interfaces*, Vol. 31, No. 1, pp. 252-257, 2009.