# Secret Image Sharing Schemes by Using Maximum Distance Separable Codes

Ching-Nung Yang, Chi-Le Hsieh, and Song-Ruei Cai

***Abstract*—A well-known polynomial-based (*k*, *n*) secret image sharing (SIS) scheme is to share a secret image into *n* noise-like shadow images, and the secret image can be recovered from any *k* shadow images. In this polynomial-based (*k*, *n*)-SIS scheme, the pixels of the secret image should be permuted to achieve the randomness of shadow images. If we do not permute secret image, there will be a problem of remanent secret image on shadow images. However, if we use a key to permute secret image then we need keeping this permutation key in advance or sharing it among all participants. In this paper, we adopt Reed Solomon code, a maximum distance separable code, to propose a (*k*, n)-SIS scheme. Our (*k*, *n*)-SIS scheme solves the problem of remanent secret image on shadows, and does not need permuting secret image. Meantime, we can reduce the shadow size like polynomial-based (*k*, *n*)-SIS that reduces shadow size to 1/*k* of secret image size.**

***Index Terms*—Secret sharing, secret image sharing, Reed Solomon (RS) code, maximum distance separable (MDS) code.**

## I. Introduction

Secret image sharing (SIS) combines methods and techniques from cryptography and image processing. So, it is an important research area and has attracted researchers in multimedia community. A SIS scheme shares a secret message into shadow images, which are referred to as shadows, in the way that if shadows are combined in a specific way, the secret image can be recovered. SIS scheme is usually implemented as a threshold (*k*, *n*)-SIS scheme, where $k \le n$, that divides a secret image into *n* shadows. By collecting any *k* shadows, we can reconstruct the secret image, but use of (*k*−1) or fewer shadows will not gain any information about the secret image.

There are two major types of SIS scheme: one is the visual cryptography (VC) and the other is the polynomial-based SIS scheme. VC has the novel stacking-to-see property where decoding requires neither knowledge of cryptography nor computer. Participants may photocopy their shared images onto transparencies and stack them to visually decode the secret through human visual system. Contrarily, the reconstructed image of polynomial-based SIS scheme is lossless, but it needs computation (Lagrange interpolation). More details of VC and polynomial-based SIS scheme, readers can refer to the book [1]. A new type of SIS scheme combining VC and polynomial-based SIS scheme with two decoding options was introduced [2]-[4]. In such scheme, one can decode secret image for preview by stacking shadows like VC when a computer is temporarily unavailable. When the computer is available during the decoding scene, we can recover the high-quality image back by using polynomial-based SIS approach.

Shamir [5] proposed a novel (*k*, *n*) secret sharing to hide a secret data in the constant term of a (*k*−1)-degree polynomial. Through Shamir's secret sharing, Thien and Lin [6] firstly proposed a polynomial-based (*k*, *n*)-SIS scheme by embedding secret pixels into all coefficients in polynomial to share the secret image and meantime reduced shadow size to 1/*k* of secret image size. Shadows in [6] are noise-like and thus suspected to censorships. Therefore, some polynomial-based (*k*, *n*)-SIS schemes were proposed using steganography so that shadows reveal meaningful images. When adding the authentication ability to detect the manipulation of shadows, this scheme is called a (*k*, *n*) steganographic and authenticated image sharing (SAIS) scheme. Based on polynomial-based (*k*, *n*)-SIS scheme, some (*k*, *n*)-SAIS schemes were proposed accordingly [7]-[11]. These (*k*, *n*)-SAIS schemes can verify the correctness of shadows to prevent accidentally generating error shadows or intentionally presenting faked shadows. Some polynomial-based SIS schemes combined with progressive recovery ability were proposed [12]-[15] to provide wide applications. Also, in [16], the authors discussed a (*k*, *n*)-SIS scheme with different importance of shadows.

From the above description, there are many researches on polynomial-based SIS scheme, and all these schemes are based on the first polynomial-based (*k*, *n*)-SIS scheme (Thien and Lin's (*k*, *n*)-SIS scheme). However, this polynomial-based (*k*, *n*)-SIS scheme needs a key to permute the pixels of secret image. If we do not permute secret image first, there will be a problem of remanent secret image on shadows.

In this paper, we adopt Reed Solomon (RS) code, a maximum distance separable (MDS) code, to propose a (*k*, *n*)-SIS scheme to solve the problem of remanent secret image on shadows. Polynomial-based SIS scheme needs a key to permute pixels in secret image before sharing, while our (*k*, *n*)-SIS scheme does not need such permutation. Meantime, our scheme can reduce the shadow size like polynomial-based (*k*, *n*)-SIS that reduces shadow size to 1/*k* of secret image size.

The rest of this paper is organized as follows. In Section II, we introduce the polynomial-based (*k*, *n*)-SIS scheme and the notion of RS code. We introduce motivation and propose a RS code based (*k*, *n*)-SIS scheme in Section III. Experiment and discussion are given in Section IV. Conclusion is drawn out in Section V.

Manuscript received May 11, 2014; revised July 17, 2014.

C. N. Yang, C. L. Hsieh, and S. R. Cai are with the CSIE Dept., National Dong Hwa University, Hualien, Taiwan (corresponding author: C. N. Yang; e-mail: cnyang@ mail.ndhu.edu.tw).

## II. Preliminaries

### A. Polynomial-Based (k, n)-SIS Scheme

Shamir firstly proposed polynomial-based ($k$, $n$) secret sharing that hides one secret data in the constant term $a_0$ of a ($k$–1)-degree polynomial $f(x)=(a_0+a_1x+...+a_{k-1}x^{k-1})$ mod $p$, where $p$ is a prime number. By using $i\in[1, n]$, a dealer can generate $n$ shadows as $S_i=(i, f(i))$, $1\le i\le n$. Any $k$ shadows (say $S_1$, $S_2$, …, $S_k$) can jointly reconstruct this ($k$–1)-degree polynomial $f(x)$ following Lagrange interpolation formula (see Eq. (1)), and the secret data can be derived from $f(0) = a_0$.

$$f(x)=\sum_{i=1}^{k} f(i)\prod_{1\le j\le k,\, j\ne i}\frac{(x-i)}{(j-i)} \bmod p. \quad (1)$$

With this ($k$–1)-degree polynomial, Thien and Lin [6] embedded secret pixels into all coefficients in $f(x)$. This polynomial-based ($k$, $n$)-SIS scheme is briefly described below. We first divide a secret image into $\tau$ non-overlapping $k$-pixel blocks, and every $j$-th ($0\le j\le\tau$–1) block includes the secret pixels ($s_{jk}$, $s_{jk+1}$, ..., $s_{jk+k-1}$). The ($k$–1)-degree polynomial $f_j(x)=(s_{jk}+s_{jk+1}x+s_{jk+2}x^2+...+s_{jk+k-1}x^{k-1}) \bmod p$ represents a shadow pixel associated with this $j$-th block, where $x$ is an image ID. By choosing $n$ shadow IDs, $i\in[1, n]$, we then obtain $n$ shadow pixels $f_j(i)$. We repeat this process for all $\tau$ blocks and generate $n$ shadows. Obviously, the shadow size will be reduced to 1/$k$ of the size of the secret image since we embed $k$ secret pixels to one shadow pixel each time.

For reconstruction, the polynomial $f_j(x)$ can be reconstructed from any $k$ shadow pixels so that we can recover the secret image. Here, we use the Galois Field $GF(2^8)$ to embed 256 grayscales in a secret image without distortion. Some polynomial-based SIS schemes adopt an ordinary arithmetic operation (i.e., mod $p$, where $p$ is 251) for simple calculation. However, under mod 251, the gray-scale values more than 250 should be truncated to 250 and this causes distortion. In this paper, we use finite field $GF(2^8)$ for this polynomial-based ($k$, $n$)-SIS scheme. Also, our RS code based ($k$, $n$)-SIS scheme is deigned over $GF(2^8)$. Finally, both schemes can recover the lossless secret image.

### B. Reed-Solomon Code

RS code is a special subclass of nonbinary BCH code. Codes of $q$-ary BCH codes for which $m$=1 are called RS codes [17]. RS codes have been widely applied on digital communication and storage systems for error control. Let $\alpha$ be a primitive element in $GF(q)$. The generator polynomial $g(x)$ of a $t$-error-correcting RS code has $\alpha$, $\alpha^2$,..., $\alpha^{2t}$ as all its roots, as shown in Eq. (2), where all elements $g_i\in GF(q)$.

$$\begin{cases} g(x)=(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t}) \\ =g_0+g_1x+g_2x^2\cdots+g_{2t-1}x^{2t-1}+g_{2t}x^{2t} \text{ (note: } g_{2t}=1). \end{cases} \quad (2)$$

Same as BCH codes, from $g(x)$, we have minimum Hamming distance $d_{min}$=(2$t$+1). Since RS code is $q$-ary BCH codes with $m$=1. So its code length is $n$=($q$–1), information length $k$=($n$–2$t$), and $d_{min}$=(2$t$+1). Notice that since $d_{min}$=(2$t$+1)=($n$–$k$+1), the value of $d_{min}$ is one greater than the number of parity-check symbols. Therefore, RS codes are also called MDS codes. Another important feature of RS code is $n$=($q$–1) that the length of the code is one less than the size of the code alphabet.

The proposed ($k$, $n$)-SIS scheme is based on systematic RS code. A systematic structure of code is that a codeword is divided into two parts, the message part and the redundant checking part. For example, for a systematic ($n$, $k$)-RS code, the message part has $k$ unaltered symbols, and the redundant checking part consists of ($n$–$k$) symbols, which are the linear sums of $k$ information symbols. The following shows how to transform $g(x)$ to a systematic generator ($k$×$n$) matrix $G$. By Eq. (2), we have ($g_0$, $g_1$, $g_2$, …, $g_{2t}$), and then put them into a rectangular array with $k$ rows and $n$ columns, as shown in Eq. (3).

$$G'=\begin{bmatrix} g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{2t} & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{2t} & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{2t} & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{2t} \end{bmatrix} \quad (3)$$

In general, $G'$ is not a systematic form. We can transfer it into a systematic form with some matrix operations. Finally, we have a matrix in systematic form $G$=[$I_k$|$P$], where $I_k$ is a $k$×$k$ unit matrix, and $P$ is $k$×($n$–$k$) parity matrix. Let $k$-tuple $\underline{u}=(u_0, u_1, ..., u_{k-1})$ be the message to be encoded, and the ($n$–$k$)-tuple $\underline{v}$ = ($v_0$, $v_1$,..., $v_{n-k-1}$) be parity digits. Then, the output codeword ($\underline{u}$||$\underline{v}$)=$\underline{u}$×$G$.

In the proposed SIS scheme, we need RS code with some specific information length and code length. Therefore, if a code of suitable code length and suitable number of information digits cannot be found, it may be desirable to shorten a code to meet the requirements. A so-called shortened ($n$–$l$, $k$–$l$)-RS code has at least the same error-correcting capability as the ($n$, $k$)-RS code. In shortened ($n$–$l$, $k$–$l$)-RS code, information symbols are deleted to obtain a desired code length and information length smaller than the design lengths.

## III. The Proposed SIS Schemes

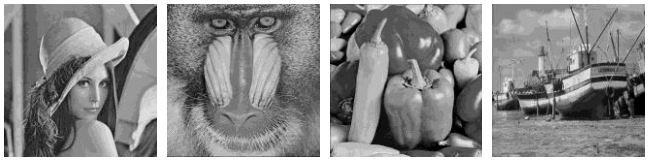
### A. Motivation

In the following example, we will show the shadows without permuting pixels for the polynomial-based ($k$, $n$)-SIS scheme.

**Example 1**: Construct the polynomial-based (2, 4)-SIS scheme without permuting pixels in secret image.

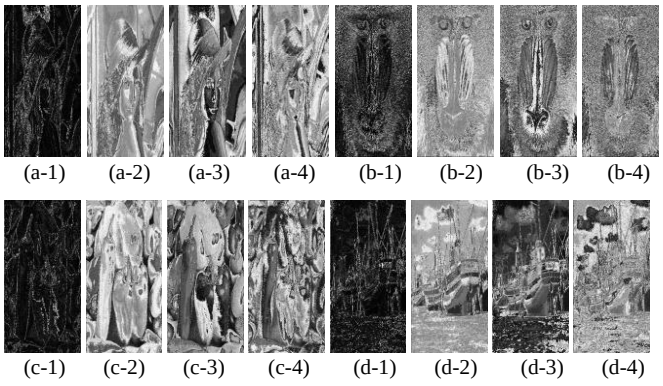
Suppose that we take 1, 2, 3 and 4 as the image IDs for four shadows $S_1$–$S_4$, and that we use the finite field $GF(2^8)$. Four secret images (512×512-pixel Lena, Baboon, Pepper, and Boat, as shown in Fig. 1) are used for testing the randomness of shadows. After applying polynomial-based (2, 4)-SIS

scheme, we have four 512×256-pixel shadows, for each secret image (see Fig. 2). In Fig. 2, it is observed that the secret image still remains on shadows, and this compromises the security. Actually, this appearance of shadow comes from the reason that small IDs used in $x^0$, $x^1$, $x^2$, …, and $x^{k-1}$ do not differ greatly. Even though some shadows using other IDs do not reveal the secret, many shadows are not completely noise-like. Some visible edges are revealed, and this is more serious (the secret image still remains on shadows) for small IDs. Finally, this causes that only some specific image IDs can be used.



(a) (b) (c) (d)

Fig. 1. Four secret images used in (2, 4)-SIS scheme: (a) Lena (b) Baboon (c) Pepper (d) Boat.



(a-1) (a-2) (a-3) (a-4) (b-1) (b-2) (b-3) (b-4)

(c-1) (c-2) (c-3) (c-4) (d-1) (d-2) (d-3) (d-4)

Fig. 2. Four shadows of (2, 4)-SIS scheme without permuting pixels in secret images: (a) Lena (b) Baboon (c) Pepper (d) Boat.

Therefore, in polynomial-based ($k$, $n$)-SIS scheme, a key is required to permute pixels in secret image, so that we can assure shadows of complete randomness and no secret revealed. In [6], the authors claimed that the key can be kept by system owner or shared among the owners of shadow images. In this paper, by using ($n$+$k$, $k$)-RS code over finite field $GF(2^8)$ instead of polynomial, we propose a ($k$, $n$)-SIS scheme without secret image remained on shadows.

### *B. The Proposed (k, n)-SIS Scheme Using RS code*

The proposed ($k$, $n$)-SIS scheme is based on systematic RS code. A systematic RS cod consists of two parts, the message part and the redundant checking part. Since the message part in a systematic code is unaltered information, we embed the secret pixels in this message part. On the other hand, the redundant checking part is the linear sums of the message part, and thus we use them for shadows. Details of shadow generation and secret reconstruction for our ($k$, $n$)-SIS scheme are outlined in Algorithm 1 and Algorithm 2, respectively.

**Algorithm 1:** Shadow generation of the proposed ($k$, $n$)-SIS scheme.

**Input:** A secret image $I$, a ($n$+$k$, $k$)-RS code over finite field $GF(2^8)$, and the systematic generator matrix $G$ of RS code.

**Output:** $n$ shadows $S_1 - S_n$.

(1) The secret image $I$ is divided into $\tau$ non-overlapping $k$-pixel blocks, and every $i$-th ($0 \le i \le \tau-1$) block is a $k$-tuple $(p_{ik}, p_{ik+1}, ..., p_{ik+k-1})$, where every pixel is the element in $GF(2^8)$.

(2) Let $G=[I_k|P]$ be the systematic generator matrix generated from $g(x)$, where $I_k$ is a $k\times k$ unit matrix and $P$ is a $k\times n$ parity matrix.
/* $G$ is publicly announce */

(3) For $i$ = 0 to $\tau$–1 do { $(p_{ik},\ldots, p_{ik+k-1} \,\|\, s_{in},\ldots, s_{in+n-1}) = (p_{ik}, \ldots, p_{ik+k-1}) \times [I_k|P]$ }.
/* we process every $k$-pixel block at each iteration, so that our shadow is the same to polynomial-based ($k$, $n$)-SIS scheme, and can reduce shadow size to 1/$k$ of secret image size */

(4) For $j$ = 1 to $n$ do $\{S_j = s_{j-1} \| s_{n+j-1} \| s_{2n+j-1} \| \cdots \| s_{(\tau-1)\times n+j-1};\}$.
/* the operation || is to concatenate the shared pixels in one shadow for constructing $n$ shadows */

**Algorithm 2:** Secret reconstruction of the proposed ($k$, $n$)-SIS scheme.

**Input:** Input any $k$ shadows out of $n$ shadows.

**Output:** the secret image $I$.

(1) Input any $k$ shadows (say $S_1$, …, $S_k$) for reconstruction.
/* for simplicity, say using $k$ shadows $S_1$, $S_2$, …, $S_k$ */

(2) Find the sub $k\times k$ matrix $G'$ from public matrix $G$.
/note: select the corresponding columns for these $k$ shadows; for this case, we select ($k$+1)-th, ($k$+2)-th, …, 2$k$-th columns from $G$ since we use $S_1$–$S_k$ for reconstruction. */

(3) Obtain all pixels $(s_{in}, \ldots, s_{in+k-1})$ from $k$ shadows involved in reconstruction.

(4) Determine the inverse matrix $[G']^{-1}$ of $G'$.

(5) For $i$ = 0 to $\tau$–1 do { $(p_{ik},\ldots, p_{ik+k-1}) = (s_{in}, \ldots, s_{in+k-1}) \times [G']^{-1}$ }.

(6) Reconstruct the secret image $I$ by restoring $\tau$ non-overlapping blocks.

**Theorem 1**: The proposed scheme is a ($k$, $n$)-SIS scheme.

**Proof**: To prove our scheme is a ($k$, $n$)-SIS scheme, we need to prove the proposed scheme satisfying two conditions: (i) the security condition that any less than $k$ shadows cannot recover any secret information (ii) the threshold property that any $k$ or more shadows can recover the secret image. We first prove the security condition.

Let a $k$-tuple in $\tau$ non-overlapping secret blocks be $\underline{u}=(u_0, u_1, \ldots, u_{k-1})$, and its corresponding shared $n$-tuple in $n$ shadows be $\underline{v}=(v_0, v_1, \ldots, v_{n-1})$, respectively, where $(\underline{u}\|\underline{v}) = \underline{u}\times G$. If we can prove that any ($k$–1) elements $(v_{i_1}, v_{i_2},\ldots, v_{i_{k-1}})$ from $\underline{v}$ cannot be used to recover the secret $\underline{u}=(u_0, u_1, \ldots, u_{k-1})$, then the security condition is satisfied. The generator $G=[I_k|P]$ is a $k\times(k+n)$ matrix with the parity matrix $P$ as shown below

$$P = \begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-1} \end{bmatrix}. \quad (4)$$

Then, from $(\underline{u}\|\underline{v})=\underline{u}\times G$, we have

$$\begin{cases} v_{i_1} = u_0 \times p_{0,i_1} + u_1 \times p_{1,i_1} + \cdots + u_{k-1} \times p_{k-1,i_1} \\ v_{i_2} = u_0 \times p_{0,i_2} + u_1 \times p_{1,i_2} + \cdots + u_{k-1} \times p_{k-1,i_2} \\ \\ v_{i_{k-1}} = u_0 \times p_{0,i_{k-1}} + u_1 \times p_{1,i_{k-1}} + \cdots + u_{k-1} \times p_{k-1,i_{k-1}} \end{cases} \quad (5)$$

From Eq. (5), we have ($k$–1) linear equations with $k$ unknowns. Thus, we cannot determine the secret ($u_0$, $u_1$, …, $u_{k-1}$).

Next, we prove that the threshold property. By the same argument, if we have $k$ or more elements ($v_{i_1}$, $v_{i_2}$,…, $v_{i_j}$), where $j \geq k$, we will have $k$ or more linear equations to correctly determine the secret ($u_0$, $u_1$, …, $u_{k-1}$).

**Lemma 1**: Suppose using (n′, k′)-RS code to construct the proposed (k, n)-SIS scheme, and we should have min{k′, (n′–k′)}≥k and (n′–k′)≥n.

**Proof**: As shown in Algorithm 1, we can use ($n$+$k$, $k$)-RS code to construct our ($k$, $n$)-SIS scheme. When applying a ($n'$, $k'$)-RS code in our scheme, we need to shorten the ($n'$, $k'$)-RS code to ($n'$–$l$, $k'$–$l$)-RS code with ($k'$–$l$)=$k$, so that the threshold property is satisfied. Therefore, we have $k' \geq k$. For this shortened ($n'$–$l$, $k'$–$l$)-RS code, we can create at most ($n'$–$k$) shadows. Obviously, we may choose any $n$ shadows out of ($n'$–$k$) shadows to construct a ($k$, $n$)-SIS scheme. Thus, we have ($n'$–$k'$)≥$n$. Since $n \geq k$ in the ($k$, $n$)-SIS scheme, so min{$k'$, ($n'$–$k'$)}≥$k$.

**Example 2**: Apply the four-error-correcting (255, 247)-RS code over $GF(2^8)$ with the primitive polynomial $1+x^2+x^3+x^4+x^8$ to implement the proposed ($k$, $n$)-SIS scheme.

From Lemma 1, this (255, 247)-RS code can be used to construct ($k$, $n$)-SIS scheme, where $k \leq \min\{247, 8\}=8$ and $n \leq 8$. So, we can use (255, 247)-RS code to construct the ($k$, 8)-SIS scheme, where $2 \leq k \leq 8$. By deleting 243 symbols from (255, 247)-RS code, we have a shortened (12, 4)-RS code. Let $\alpha$ be a primitive element in $GF(2^8)$. Then, the generator polynomial $g(x)$ of (12, 4)-RS code has $\alpha$, $\alpha^2$, $\alpha^3$, $\alpha^4$, $\alpha^5$, $\alpha^6$, $\alpha^7$, $\alpha^8$ as all its roots; hence we have

$$\begin{cases} g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5) \\ (x+\alpha^6)(x+\alpha^7)(x+\alpha^8) = \alpha^{36} + \alpha^{203}x + \alpha^3 x^2 + \\ \alpha^{220}x^3 + \alpha^{253}x^4 + \alpha^{211}x^5 + \alpha^{240}x^6 + \alpha^{176}x^7 + x^8. \end{cases} \quad (6)$$

The systematic generator matrix $G$ is derived in Eq. (7).

$$\begin{cases} G = \begin{bmatrix} \alpha^{36} & \alpha^{203} & \alpha^3 & \alpha^{220} & \alpha^{253} & \alpha^{211} & \alpha^{240} & \alpha^{176} & 1 & 0 & 0 & 0 \\ 0 & \alpha^{36} & \alpha^{203} & \alpha^3 & \alpha^{220} & \alpha^{253} & \alpha^{211} & \alpha^{240} & \alpha^{176} & 1 & 0 & 0 \\ 0 & 0 & \alpha^{36} & \alpha^{203} & \alpha^3 & \alpha^{220} & \alpha^{253} & \alpha^{211} & \alpha^{240} & \alpha^{176} & 1 & 0 \\ 0 & 0 & 0 & \alpha^{36} & \alpha^{203} & \alpha^3 & \alpha^{220} & \alpha^{253} & \alpha^{211} & \alpha^{240} & \alpha^{176} & 1 \end{bmatrix} \\ = \begin{bmatrix} 1 & 0 & 0 & 0 & \alpha^{156} & \alpha^{198} & \alpha^{25} & \alpha^{14} & \alpha^{177} & \alpha^{84} & \alpha^{40} & \alpha^{238} \\ 0 & 1 & 0 & 0 & \alpha^{19} & \alpha^{222} & \alpha^{64} & \alpha^{176} & \alpha^{251} & \alpha^{245} & \alpha^{182} & \alpha^{193} \\ 0 & 0 & 1 & 0 & \alpha^{229} & \alpha^{136} & \alpha^{139} & \alpha^{11} & \alpha^{209} & \alpha^{115} & \alpha^{139} & \alpha^{131} \\ 0 & 0 & 0 & 1 & \alpha^{167} & \alpha^{222} & \alpha^{184} & \alpha^{217} & \alpha^{175} & \alpha^{204} & \alpha^{140} & \alpha^{219} \end{bmatrix} \\ = \begin{bmatrix} 1 & 0 & 0 & 0 & 228 & 7 & 3 & 19 & 219 & 107 & 106 & 11 \\ 0 & 1 & 0 & 0 & 90 & 138 & 95 & 227 & 216 & 233 & 98 & 25 \\ 0 & 0 & 1 & 0 & 122 & 79 & 66 & 232 & 162 & 124 & 66 & 92 \\ 0 & 0 & 0 & 1 & 126 & 138 & 149 & 155 & 255 & 221 & 132 & 86 \end{bmatrix} \text{ (decimal format).} \end{cases} \quad (7)$$

The proposed (4, 8)-SIS scheme can be constructed from the shortened (12, 4)-RS code. Suppose one 4-pixel secret block is $\underline{u}$ = (5, 2, 7, 10), and then we have ($\underline{u}||\underline{v}$) = $\underline{u}\times G$. The values of $\underline{v}$ = (183, 207, 137, 161, 60, 125, 137, 186). Repeat processing all non-overlapping 4-pixel blocks. Finally, we can generate 8 shadows. In Polynomial-based SIS scheme, every shadow has its own image ID. The proposed scheme also needs an image ID for each shadow, i.e., we deliver the $i$-th shadow value in $\underline{v}$ to the shadow $S_i$, $1 \leq i \leq 8$. For example, we may deliver the third shared value "137" in $\underline{v}$ to the shadow $S_3$. For reconstruction, suppose that 4 shadows $\{S_1, S_4, S_5, S_8\}$ are involved in recovering the secret. Here, we show how to recover a 4-pixel secret block. From shadows, we have 4 shadow values (183, 161, 60, 186). We first find the inverse matrix $\left(\begin{bmatrix} 228 & 19 & 219 & 11 \\ 90 & 227 & 216 & 25 \\ 122 & 232 & 162 & 92 \\ 126 & 155 & 255 & 86 \end{bmatrix}\right)^{-1} = \begin{bmatrix} 239 & 50 & 24 & 99 \\ 35 & 94 & 53 & 220 \\ 222 & 173 & 225 & 173 \\ 143 & 226 & 126 & 141 \end{bmatrix}$. By Eq. (8), we can determine the secret $\underline{u}$ = ($u_1$, $u_2$, $u_3$, $u_4$) = (5, 2, 7, 10).

$$(183, 161, 60, 186) \times \begin{bmatrix} 239 & 50 & 24 & 99 \\ 35 & 94 & 53 & 220 \\ 222 & 173 & 225 & 173 \\ 143 & 226 & 126 & 141 \end{bmatrix} = (5,\ 2,\ 7,\ 10). \quad (8)$$

In Table I, we show $g(x)$ and $G$ for four shortened ($n'$, $k'$)-RS codes, on which four ($k$, $n$)-SIS schemes (2, 6)-SIS scheme, (3, 8)-SIS scheme, (4, 10)-SIS scheme, and (5, 12)-SIS scheme) are constructed.

TABLE I: ($k$, $n$)-SIS SCHEMES BASED ON ($k'$, $n'$) SHORTENED CODES

| $n'$ | $k'$ | $n$ | $k$ | $g(x)$ | $G$ |
|---|---|---|---|---|---|
| 8 | 2 | 6 | 2 | $(x+\alpha)(x+\alpha^2)(x+\alpha^3)$ $(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$ | $\begin{bmatrix} 1 & 0 & 195 & 170 & 190 & 143 & 241 & 66 \\ 0 & 1 & 230 & 125 & 248 & 203 & 154 & 251 \end{bmatrix}$ |
| 11 | 3 | 8 | 3 | $(x+\alpha)(x+\alpha^2)(x+\alpha^3)$ $(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$ $(x+\alpha^7)(x+\alpha^8)$ | $\begin{bmatrix} 1 & 0 & 0 & 90 & 138 & 95 & 227 & 216 & 233 & 98 & 25 \\ 0 & 1 & 0 & 122 & 79 & 66 & 232 & 162 & 124 & 66 & 92 \\ 0 & 0 & 1 & 126 & 138 & 149 & 155 & 255 & 221 & 132 & 86 \end{bmatrix}$ |
| 14 | 4 | 10 | 4 | $(x+\alpha)(x+\alpha^2)(x+\alpha^3)$ $(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$ $(x+\alpha^7)(x+\alpha^8)(x+\alpha^9)$ $(x+\alpha^{10})$ | $\begin{bmatrix} 1 & 0 & 0 & 0 & 80 & 68 & 65 & 73 & 164 & 18 & 61 & 129 & 120 & 116 \\ 0 & 1 & 0 & 0 & 190 & 90 & 197 & 166 & 248 & 201 & 29 & 239 & 113 & 248 \\ 0 & 0 & 1 & 0 & 179 & 107 & 113 & 25 & 36 & 238 & 248 & 140 & 216 & 110 \\ 0 & 0 & 0 & 1 & 88 & 35 & 76 & 117 & 153 & 116 & 54 & 19 & 141 & 28 \end{bmatrix}$ |
| 17 | 5 | 12 | 5 | $(x+\alpha)(x+\alpha^2)(x+\alpha^3)$ $(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$ $(x+\alpha^7)(x+\alpha^8)(x+\alpha^9)$ $(x+\alpha^{10})(x+\alpha^{11})(x+\alpha^{12})$ | $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 157 & 165 & 61 & 24 & 28 & 232 & 37 & 255 & 134 & 137 & 74 & 249 \\ 0 & 1 & 0 & 0 & 0 & 74 & 81 & 248 & 187 & 127 & 218 & 144 & 143 & 148 & 63 & 153 & 148 \\ 0 & 0 & 1 & 0 & 0 & 248 & 25 & 248 & 83 & 236 & 2 & 15 & 100 & 236 & 214 & 132 & 140 \\ 0 & 0 & 0 & 1 & 0 & 204 & 99 & 131 & 175 & 79 & 98 & 254 & 87 & 149 & 185 & 167 & 205 \\ 0 & 0 & 0 & 0 & 1 & 223 & 90 & 222 & 202 & 204 & 212 & 62 & 35 & 201 & 138 & 3 & 219 \end{bmatrix}$ |

## IV. EXPERIMENT AND DISCUSSION

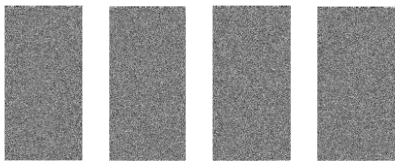
### A. Experimental Results

We conduct an experiment to test the randomness of shadows. The proposed (2, 4)-SIS scheme based on shortened (8, 2)-RS code with the systematic generator matrix $G$ in Eq. (8) (from Table I). This (8, 2)-RS code can be used to construct (2, $n$), where $2 \leq n \leq 6$. To compare polynomial-based (2, 4)-SIS scheme in Example 1, we construct (2, 4)-SIS scheme using the first four columns in parity matrix $P$ of the following $G$ matrix.

$$G = \begin{bmatrix} 1 & 0 & 195 & 170 & 190 & 143 & 241 & 66 \\ 0 & 1 & 230 & 125 & 248 & 203 & 154 & 251 \end{bmatrix} \quad (8)$$

Suppose that Lena in Fig. 1(a) is used as the secret image, Fig. 3 shows four shadows ($S_1$–$S_4$) with the size 512×256

pixels. The shadow size is half reduced. When compared with the shadows of polynomial-based (2, 4)-SIS scheme (see Fig. 2(a)), the shadows in Fig. 3 are completely noise-like. However, Lena can be revealed from shadows in Fig. 2(a).



(a) $S_1$ (b) $S_2$ (c) $S_3$ (d) $S_4$

Fig. 3. Four shadows of the proposed (2, 4)-SIS scheme using (8, 2)-RS code.

### B. Discussion

In polynomial-based ($k$, $n$)-SIS scheme, if we do not permute the pixels in secret image, many shadows are not completely noise-like. Some visible edges on shadow images are revealed, and this causes that only some specific image IDs can be used. For small image IDs, the secret even will be revealed. Therefore, using a permutation key is necessarily required in polynomial-based SIS scheme. In [6], the authors propose two possible approaches for delivering this key. One is that the key can be kept by the system owner. For this case, the system owner should be involved in reconstruction phase. This is, strictly speaking, not a secret sharing scheme. A ($k$, $n$) secret sharing scheme should provide the threshold property, i.e., only $k$ shadows are required for reconstructing the secret. The second approach is that the key is shared among the owners of shadows. Thus, the key is either delivered to each participant or shared among all participants by using secret sharing again. If the dealer delivers this key to all participants, then an extra key distribution protocol is needed. Certainly, the dealer can share the permutation key by secret sharing again. Then, each shadow contains not only the shared information of secret but also the information of key.

In polynomial based ($k$, $n$)-SIS scheme, in fact, the problem of remanent secret images on shadows comes from small IDs used in $x^0$, $x^1$, $x^2$, …, and $x^{k-1}$ (note: we embed secret pixels in coefficients of ($k$−1)-degree polynomial) do not differ greatly. In this paper, our ($k$, $n$)-SIS scheme uses RS code and does not use the polynomial. Although our scheme also needs the image IDs, i.e., which column we use for shadow, this image ID is not involved in calculating the shadow values. Thus, we do not need permuting secret image to prevent the problem of remanent secrete image.

## V. Conclusion

We consider how to solve the problem of remanent secret image on shadows. Polynomial-based SIS scheme adopts a trivial solution that permutes pixels in secret image before sharing procedure. In this paper, we solve this problem and propose a ($k$, $n$)-SIS scheme by using ($n$+$k$, $k$)-RS code. Our ($k$, $n$)-SIS scheme can achieve the threshold property, and meantime reduces the shadow size like polynomial-based ($k$, $n$)-SIS that reduces shadow size to 1/$k$ of secret image size.

## Acknowledgment

This work was supported in part by National Science Council, by NSC under Grant 102-2221-E-259 -009-MY2 and 102-2218-E-259 -006.

## References

[1] S. Cimato, and C. N. Yang, *Visual cryptography and secret image sharing*, CRC Press, Taylor & Francis, 2011.

[2] S. J. Lin, and J. C. Lin, "VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," *Pattern Recognition*, vol. 40, pp. 3652-3666, 2007.

[3] C. N. Yang and C. B. Ciou, "Image secret sharing method with two-decoding-options: lossless recovery and previewing capability," *Image and Vision Computing*, vol. 28, pp. 1600-1610, 2010.

[4] P. Li, P. J. Ma, X. H. Su, and C. N. Yang, "Improvements of a two-in-one image secret sharing scheme based on gray mixing model," *Journal of Visual Communication and Image Representation*, vol. 23, pp. 441-453, 2012.

[5] A. Shamir, "How to share a secret", *Communications of the Association for Computing Machinery*, vol. 22, pp. 612-613, 1979.

[6] C. C. Thien and J. C. Lin, "Secret image sharing," *Computer & Graphics*, vol. 26, pp. 765-770, 2002.

[7] C. C. Lin, and W. H. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, pp. 405-414, 2004.

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

[9] C. N. Yang, and C. B. Ciou, "A comment on "sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 42, pp. 615-1619, 2009.

[10] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme," *Journal of Systems and Software*, vol. 84, pp. 2196-2207, 2011.

[11] C. N. Yang, J. F. Ouyang, and L. Harn, "Steganography and authentication in image sharing without parity bits," *Optics Communications*, vol. 285, pp. 1725-1735, 2012.

[12] R. Z. Wang and S. J. Shyu, "Scalable secret image sharing," *Signal Processing: Image Communication*, vol. 22, pp. 363-373, 2007.

[13] Y. Y. Lin and R. Z. Wang, "Scalable secret image sharing with smaller shadow image," *IEEE Signal Processing Letters*, vol. 17, pp. 316-319, 2010.

[14] C. N. Yang and S. M. Huang, "Constructions and properties of k out of n scalable secret image sharing," *Optics Communications*, vol. 283, pp. 1750-1762, 2010.

[15] C. N. Yang and Y. Y. Chu, "A general ($k$, $n$) scalable secret image sharing scheme with the smooth scalability," *Journal of System and Software*, vol. 84, pp. 1726-1733, 2011.

[16] P. Li, C. N. Yang, C. C. Wu, Q. Kong, and Y. Ma, "Essential secret image sharing scheme with different importance of shadows", *Journal of Visual Communication and Image Representation*, vol. 24, pp. 1106-1114, 2013 .

[17] S. Lin and D. J. Costello, *Error control coding*, Pearson Prentice Hall, 2004.

**Ching-Nung Yang** received the B.S. degree in 1983 and the M.S. degree in 1985, both from the Department of Telecommunication Engineering at National Chiao Tung University. He received the Ph.D. degree in electrical engineering from National Cheng Kung University in 1997. During 1987-1989 and 1990-1999, he worked at the Telecommunication Lab. and Training Institute Kaohsiung Center, Chunghwa Telecom Co., Ltd., respectively. He is presently a full professor at the Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan. He is also an IEEE senior member. His research interests include coding theory, information security, and cryptography.

**Chi-Le Hsieh** is a graduate student at the Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan. His research includes information security and secret image sharing.

**Song-Ruei Cai** is a graduate student at the Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan. His research includes visual cryptography and secret image sharing.