Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 418090, 7 pages
http://dx.doi.org/10.1155/2014/418090

Research Article

Nonlinear Secret Image Sharing Scheme

Sang-Ho Shin, Gil-Je Lee, and Kee-Young Yoo

School of Computer Science and Engineering, Kyungpook National University, 80 Daehakro, Bukgu, Daegu 702-701, Republic of Korea

Correspondence should be addressed to Kee-Young Yoo; yook@knu.ac.kr

Received 14 February 2014; Revised 17 June 2014; Accepted 28 June 2014; Published 21 July 2014

Academic Editor: Long Cheng

Over the past decade, most of secret image sharing schemes have been proposed by using Shamir's technique. It is based on a linear combination polynomial arithmetic. Although Shamir's technique based secret image sharing schemes are efficient and scalable for various environments, there exists a security threat such as Tompa-Woll attack. Renvall and Ding proposed a new secret sharing technique based on nonlinear combination polynomial arithmetic in order to solve this threat. It is hard to apply to the secret image sharing. In this paper, we propose a (t, n)-threshold nonlinear secret image sharing scheme with steganography concept. In order to achieve a suitable and secure secret image sharing scheme, we adapt a modified LSB embedding technique with XOR Boolean algebra operation, define a new variable m, and change a range of prime p in sharing procedure. In order to evaluate efficiency and security of proposed scheme, we use the embedding capacity and PSNR. As a result of it, average value of PSNR and embedding capacity are 44.78 (dB) and $1.74t \lceil \log_2 m \rceil$ bit-per-pixel (bpp), respectively.

1. Introduction

In a security system, there is a maintenance tool which must be checked every day. In order to check it, someone must have access to this system. Three senior administrators are engaged, but they do not trust the combination to any individual administrator. Hence, we would like to design a system whereby any two of three administrators can gain access to this system, but an individual administrator cannot do so. In order to design this system, we adapt a concept of secret sharing. A secret sharing is technique for distributing a secret amongst a group of honest participants, and each secret piece is allocated for each participant after the secret is divided into several pieces. This secret can be reconstructed only when a sufficient number, of possibly different types of shares are combined together; an individual share is no use on its own [1–3]. Blakley [4] and Shamir [5] have proposed a concept of secret sharing for the first time. It is that the secret is divided into n shares for n participants, and t is used as a threshold value ($t \leq n$). It was called a (t, n)-threshold technique and it means that at least t participants of n participants should be gathered.

With the development of computing and network technologies, in the meantime, multimedia data such as image, audio, and video files have transmitted over the Internet, actively. As a result, multimedia security has emerged as an important issue [6–14]. In 2002, Thien and Lin [15] have proposed a (t, n)-threshold secret image sharing scheme for the first time. The secret image can be shared by several shadow images so the size of each shadow image is only $1/t$ of that of the secret image for convenient hiding, storage, and transmission in their scheme. Lin and Tsai [16] have proposed a secret image sharing with steganography concept based on the Shamir's (t, n)-threshold scheme. By using the parity bit check method, they claimed that their scheme can prevent from incidentally bringing an erroneous shadow image or intentionally providing a false image to achieve the authentication goal. They also presented another user-friendly image sharing such that shadow images look like natural images [17]. Recently, Lin and Chan [18] proposed a reversible secret image sharing scheme in 2010. They have achieved a low distortion and high embedding capacity. Additionally, it can reconstruct the secret and cover images, completely.

As mentioned above, most of secret image sharing schemes are based on Shamir's (t, n)-threshold. It has utilized a linear combination polynomial arithmetic in sharing procedure. A configuration of the linear combination polynomial with (t, n) is as follows:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}. \quad (1)$$

In sharing procedure for n participants, an arbitrary share k_i ($1 \le i \le n$) is computed by above function $f(x)$. Each share k_i is distributed to participant i. In order to reconstruct the secret, we need t pairs of (i, k_i). In this procedure, an arbitrary participant can submit a false share and only he will be able to obtain the correct secret while leaving the others with the incorrect secret. It is called a Tompa-Woll attack [19, 20]. This attack is caused by the linear property. Renvall and Ding [21] have proposed a new secret sharing scheme based on a nonlinear combination polynomial arithmetic in order to solve this problem. The nonlinear combination arithmetic indicates an inner product for any arbitrary matrix [21]. However, it is hard to apply to the secret image sharing.

In this paper, we propose a nonlinear secret image sharing scheme with steganography concept. Although the proposed scheme is based on Renvall and Ding's sharing and reconstruction methods [21], we adapt several new techniques in order to achieve a suitable and secure secret image sharing scheme. In sharing procedure, we define a new variable m and change a range of prime p in order to attain the prevention of overflow (or underflow) and reinforce the security. Also, we propose a modified LSB embedding technique with XOR Boolean algebra operation in order to get the high embedding capacity. In order to evaluate efficiency and security of proposed scheme, we use the embedding capacity and PSNR. As the experimental results, we analyze the efficiency and security between proposed and previous techniques.

This paper is organized as follows. Section 2 introduces Shamir's and Renvall and Ding's secret sharing scheme. Considerations and algorithm of proposed scheme are discussed in Section 3. Section 4 presents the experimental results. Lastly, Section 5 gives the conclusions.

2. Preliminaries

In this section, Shamir's (t, n)-threshold secret sharing and Renvall and Ding's nonlinear secret sharing are introduced.

2.1. Shamir's (t, n)-Threshold Secret Sharing. In 1979, Shamir has proposed a secret sharing scheme for the first time [5]. It is based on (t, n)-threshold which is defined as follows [2].

Definition 1. Let t, n be positive integers and $t \le n$. A (t, n)-*threshold* is a method of sharing a *key* K among a set of n participants (denoted by $\mathcal{P}$), in such a way that any t participants can compute the value of K, but no group of $t-1$ participants can do so.

For the example of $(2, 3)$-threshold, the value of K is chosen by a honest participant called the *dealer* (denoted by D, $D \notin \mathcal{P}$, where $\mathcal{P}$ is a set of participants). If D wants to share K among the participants in $\mathcal{P}$, D distributes some partial information of K (called a *share*) for each participant. The shares should be distributed secretly, so no participant knows the share given to another participant. That is, an arbitrary participant does not know the information of K in $(2, 3)$-threshold. In order to reconstruct a K, two or more participants should get together by an arbitrary algorithm.

In Shamir's scheme, the linear combination polynomial and Lagrange's interpolation arithmetic operations over prime p were used in order to distribute and reconstruct a K, respectively. It consists of three phases with (t, n)-threshold: initialization, share distribution, and reconstruction.

2.1.1. Initialization Phase. D chooses n distinctly nonzero elements of $\mathbb{Z}_p$, denoted by x_i, $1 \le i \le n$ (where $p \ge n + 1$). For $1 \le i \le n$, D gives the value x_i to P_i. The value x_i is public.

2.1.2. Share Distribution Phase. When D wants to share a key $K \in \mathbb{Z}_p$, D secretly chooses $t-1$ elements of $\mathbb{Z}_p$ which are denoted as $a_1, \ldots, a_{t-1}$. And then D computes $y_i = f(x_i)$, for $1 \le i \le n$, by

$$y_i = f(x_i) = K + \sum_{j=1}^{t-1} a_j x_i^j \pmod{p}, \tag{2}$$

where $a_1, a_2, \ldots, a_{t-1}$ are randomly determined from integers within $[0, p-1]$. Finally, D distributes the share y_i to P_i.

2.1.3. Reconstruction Phase. If participants want to reconstruct a K, t or more participants will be recruited by D. K is reconstructed with information $(x_i, f(x_i))$ for each participant P_i and Lagrange interpolation formula as shown in (3) for polynomials.

Consider

$$f(x) = \sum_{j=1}^{t} \left(y_i, \prod_{1 \le k \le t, k \ne j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \bmod p. \tag{3}$$

Lastly, a key can be derived from $f(0) = K$.

2.2. Renvall and Ding's $(t-1, n)$-Threshold Nonlinear Secret Sharing. In 1996, Renvall and Ding [21] have proposed a nonlinear secret sharing scheme. A polynomial arithmetic technique is based on quadratic form (called a nonlinear combination) instead of the linear combination. In fact, it is an inner product for an arbitrary matrix, and detailed arithmetic is as follows [21].

Let p be a large prime of the form $p \equiv 3 \pmod 4$. In order to generate the secret, it should be within $[0, (p-1)/2]$. All arithmetic operations are performed over Galois field (GF(p)). For any positive integers t, n ($t \le n$) and each set of indices $1 \le i_1 < \cdots < i_t \le n$, Vandermonde matrix $\mathtt{M}$ is generated by

$$\mathtt{M} = \begin{pmatrix} (a_{i_1})^0 & (a_{i_1})^1 & \cdots & (a_{i_1})^{t-1} \\ (a_{i_2})^0 & (a_{i_2})^1 & \cdots & (a_{i_2})^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ (a_{i_t})^0 & (a_{i_t})^1 & \cdots & (a_{i_t})^{t-1} \end{pmatrix}, \tag{4}$$

where all elements in matrix $\mathtt{M}$ are distinct nonzero over GF(p) and $\mathtt{M}$ must satisfy two requirements as follows.

R1: for any set of indices $1 \le i_1 < \cdots < i_{t-1} \le n$,

$$1 + \sum_{u=1}^{t-1} \left(\sum_{v=1}^{t-2} N \right)^2 \ne 0, \tag{5}$$

where $\mathtt{N} = [n(i_1, i_2, \ldots, i_{t-1})_{u,v}]$ is the inverse of $\mathtt{M}$ by the Chinese remainder algorithm.

R2: for any set of indices $1 \le i_1 < \cdots < i_{t-2} \le n$, one of the following conditions is held:

(1) $\delta \neq 0$ and $\delta^2 - 4\beta\gamma$ is a quadratic residue,

(2) $\delta = 0$, $\gamma \neq 0$, and $-\beta/\gamma$ is a quadratic residue,

where β, δ, and γ are expressed by (6), (7), and (8), respectively.

Consider

$$\beta = 1 + \sum_{u=1}^{t-1}\left(\sum_{v=1}^{t-2} n(i_1, i_2, \ldots, i_{t-1})_{u,v}\right)^2, \tag{6}$$

$$\gamma = 1 + \sum_{u=1}^{t-1}\left(\sum_{v=1}^{t-2} n(i_1, i_2, \ldots, i_{t-1})_{u,v}\left(a_{i_t}\right)^{t-1}\right)^2, \tag{7}$$

$$\delta = 2\sum_{u=1}^{t-2}\left(\sum_{v=1}^{t-2}\mathtt{N}\right)\left(\sum_{v=1}^{t-2}\mathtt{N}\left(a_{i_t}\right)^{t-1}\right), \tag{8}$$

where $\mathtt{N} = [n(i_1, i_2, \ldots, i_{t-1})_{u,v}]$.

In sharing process, the secret s_1 with $0 \le s_1 \le (p-1)/2$ is selected to be shared among n participants. Then, $s_2, \ldots, s_t$ are randomly chosen over GF(p). Let a set $\mathbf{s} = \{s_1, s_2, \ldots, s_t\}$. Each share is calculated by

$$f(\mathbf{x}) = \mathbf{x}\mathbf{x}^T = (x_1)^2 + (x_2)^2 + \cdots + (x_t)^2 \quad \text{over GF}(p), \tag{9}$$

where $\mathbf{x}$ is a row vector (or row matrix which has a single row of t elements) and it can be expressed as $\mathbf{x} = [x_1\ x_2 \cdots x_t]$, and $\mathbf{x}^T$ is a transpose of $\mathbf{x}$.

In order to distribute the shares, D calculates k_0 and k_{i_j} as follows:

$$k_0 = f(s) = (s_1)^2 + \cdots + (s_t)^2,$$

$$k_i = f\left(s + \alpha_{i_j}\right) = \left(s_1 + \left(a_{i_1}\right)^0\right)^2 + \cdots + \left(s_t + \left(a_{i_1}\right)^{t-1}\right)^2, \tag{10}$$

where α_{i_j} is i_jth row vector in a Vandermonde matrix $\mathtt{M}$ (as shown in (4)) and $1 \le i_j \le n$. Then D distributes (k_0, k_{i_j}) to participant P_{i_j}.

If participants want to reconstruct the secret s, $t-1$ or more participants will be recruited by D. And then, s_1 is reconstructed with information (k_0, k_{i_j}) for each participant P_{i_j} and as follows:

$$k_0 = f(\mathbf{s}), \qquad k_{i_j} - k_0 = 2\alpha_{i_j}\mathbf{s}^T + \alpha_{i_j}\alpha_{i_j}^T. \tag{11}$$

They have completed verification of security for Tompa-Woll attack [21]. In this paper, we propose a nonlinear secret image sharing based on concepts of their scheme and steganography.

3. The Proposed Scheme

In this section, we illustrate considerations, sharing, and reconstruction algorithms.

3.1. Considerations. In order to propose a new nonlinear secret image sharing scheme, we discuss some considerations such as handing techniques of secret and shadow images and overflow (or underflow).

3.1.1. Handling of Secret Image. In previous scheme, they used $(t-1, n)$-threshold concept. But we adapt a concept of (t, n)-threshold because of the convenience of proposed scheme. Given (t, n)-threshold, we require that the secret image (SI) to be divided into n shadow images (SHIs), and SI cannot be reconstructed without t or more SHIs. However, secrets $(s_1, s_2, \ldots, s_t)$ are generated from SI's pixel values. The major difference between proposed and Renvall and Ding's schemes is that random value does not use $s_2, \ldots, s_t$. Also, the range of prime p should be at least 60 bits in their scheme, but we let the range be $2 \le p \le 251$. Tompa-Woll attack can occur because the range of prime p is less than 60 bits. But, our scheme is safe for this attack because it is based on the steganography concept that the secret is hidden in friendly cover image such as Lena, airplane, and baboon.

3.1.2. Overflow and Underflow. If an arbitrary pixel value in SI is one of 251 to 255, it can occur an overflow or underflow because all arithmetic operations are performed within GF(251). So, we define another variable positive integer m $(2 \le m \le p)$ in order to prevent overflow or underflow. A pixel value in SI is converted by m-ary form. For example, if a pixel value and m are $160_{(10)}$ and 7, respectively, converted pixel value is $316_{(7)}$. This converting technique is to provide reinforcement of security robustness. The converted m-ary values utilize inputs of nonlinear polynomial arithmetic. And then, its outputs are performed with modulo-p operation. Even if an attacker knows sharing and reconstruction algorithm of the proposed scheme, it is difficult to extract the correct SI.

3.1.3. The Generation of Shadow Image. In Renvall and Ding's scheme, (k_0, k_{i_j}) is just a shadow. It was distributed to the participant P_{i_j} by the dealer D. However, the shadow is an image that (k_0, k_{i_j}) is embedded in the proposed scheme. In order to generate the shadow image, hence, we utilize XOR Boolean algebra operation for k_0 and k_{i_j}.

3.2. Sharing Procedure. Suppose that the cover image (CI), shadow image (SHI), and secret image (SI) consist of $M \times M$, $M \times M$ and $N \times N$ pixels, and these represent CI $= \{C_0, C_1, \ldots, C_{M^2-1}\}$, SHI $= \{\mathrm{SH}_0, \mathrm{SH}_1, \ldots, \mathrm{SH}_{M^2-1}\}$, and SI $= \{S_0, S_1, \ldots, S_{N^2-1}\}$, respectively. In order to determine the number of participants, the dealer (D) decides to fix the

Table 1: The embedding method by prime p.

Range	Embedding technique	Pixel block
$2^0 < p \le 2^1$	LSB1	per 1 pixel
$2^1 < p \le 2^2$	LSB2	per 1 pixel
$2^2 < p \le 2^3$	LSB1 and LSB2	per 2 pixels
$2^3 < p \le 2^4$	LSB2	per 2 pixels
$2^4 < p \le 2^5$	LSB1 and LSB2	per 3 pixels
$2^5 < p \le 2^6$	LSB2	per 3 pixels
$2^6 < p \le 2^7$	LSB1 and LSB2	per 4 pixels
$2^7 < p \le 2^8$	LSB2	per 4 pixels

threshold values t and n ($t \le n$). Also, D securely chooses a prime p and positive integer m ($m \le p$).

In this procedure, the sharing process is described.

Input: A CI with size of $M \times M$ and a SI with size of $N \times N$.

Output: n SHIs with size of $M \times M$.

Step 1. Convert a ith pixel value (S_i) in SI into m-ary's expression as follows:

$$S_i \Longrightarrow \left\{s_{i\lceil \log_m 255\rceil}, \ldots, s_{(i+1)\lceil \log_m 255\rceil - 1}\right\}, \tag{12}$$

where $0 \le i \le N^2 - 1$ and $m \le p$. For example, if m is 3, s_i is one of 0, 1, or 2. Let a set $\mathbf{S}$ consist of r subsets that compose tm-ary's values and it is expressed by

$$\mathbf{S} = \left\{\mathbf{s}^0 = \left(s_0, \ldots, s_{t-1}\right), \mathbf{s}^1 = \left(s_t, \ldots, s_{2t-1}\right), \ldots, \mathbf{s}^{r-1}\right\}. \tag{13}$$

If $(N^2 - 1)\lceil \log_m 255\rceil$ is not a multiple of t, the remaining part in the last subset s^{r-1} is filled by using well-known padding techniques.

Step 2. Choose $\boldsymbol{\alpha}_j = ((a_j)^0, (a_j)^1, (a_j)^2, \ldots, (a_j)^{t-1})$ for all participants by D, where $a_j \in \mathrm{GF}(p)$ and $1 \le j \le n$. For any t participants, the matrix $\mathtt{M}$ which satisfies two requirements R1 and R2 is constructed as (14) in order to ensure the correctly selected $\boldsymbol{\alpha}_j$. If $\mathtt{M}$ does not satisfy two requirements, D should select a new $\boldsymbol{\alpha}_j$. Also, $\mathtt{M}$ will be used in the reconstruction procedure.

Consider

$$\mathtt{M} = \begin{pmatrix} \boldsymbol{\alpha}_1 \\ \boldsymbol{\alpha}_2 \\ \vdots \\ \boldsymbol{\alpha}_t \end{pmatrix}. \tag{14}$$

Step 3. Calculate a shadow value $k_j^l = f(\mathbf{s}^l + \boldsymbol{\alpha}_j)$ (where $k_j^0 = f(\mathbf{s}^0)$, $1 \le j \le n$ and $1 \le l \le r - 1$) with $f(\mathbf{x})$ (as shown in (9)) and $\mathbf{S}$ and $\boldsymbol{\alpha}_j$ by D.

Step 4. Embed the generated lth shadow value ($k_j^0 \oplus k_j^l$) for j-th participant into CI with LSB1 and LSB2 techniques by Table 1 in order to generate SHI_j ($1 \le l \le r - 1$ and $1 \le j \le n$). "$\oplus$" indicates XOR Boolean algebra operation. Table 1 shows the embedding method by prime p. For example, it corresponds to the range of $2^4 < p \le 2^5$ when p is 19. Hence, $k_j^0 \oplus k_j^l$ are embedded by LSB1 and LSB2 techniques for 3 pixels.

Step 5. Distribute the generated SHI_j into jth participant by D. And then, D stores k_j^0 ($1 \le j \le n$) for all s^l ($0 \le l \le r - 1$).

3.3. Reconstruction Procedure. In this procedure, the reconstruction process is described.

Input: t SHI_js with size of $M \times M$.

Output: a reconstructed SI' with size of $N \times N$.

Step 1. Extract a lth shadow value ($k_j^0 \oplus k_j^l$) from jth participant's SHI_j ($1 \le l \le r - 1$ and $1 \le j \le k$), and k_j^l by XOR Boolean operation $(k_j^0 \oplus k_j^l) \oplus k_j^0$.

Step 2. Calculate a lth converted m-ary's value $\mathbf{s}^l$ ($0 \le l \le r - 1$) as follows:

$$\begin{aligned} k_j^0 &= f\left(\mathbf{s}^0\right), \qquad k_j^l = f\left(\mathbf{s}^l + \alpha_j\right), \\ k_j^0 &= f\left(\mathbf{s}^0\right), \qquad k_j^l - k_j^0 = 2\alpha_j\left(\mathbf{s}^l\right)^T + \alpha_j\alpha_j^T. \end{aligned} \tag{15}$$

Step 3. Convert the calculated $s_0, s_1, \ldots, s_{(N^2-1)\lceil \log_m 255\rceil}$ into pixel values by m, and, reconstruct a SI' with size of $N \times N$.

4. Experimental Results

In this section, we analyze the security and efficiency of proposed scheme.

4.1. The Measurement Tools. In order to estimate the efficiency and security of secret image sharing schemes, there exist two typical measurement tools: the embedding capacity and PSNR. The embedding capacity means the amount of embedded secret data in a cover image, and it can evaluate the efficiency of secret image sharing technique. That is, if the embedding capacity of an arbitrary technique is more increased, we can say that this technique has a good efficiency. It is generally measured in bit-per-pixel (bpp) or bit.

PSNR is the abbreviation for "*peak signal-to-noise ratio*" and it is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Nowadays, PSNR is the most popular distortion measurement tool in the field of image and video coding and compression. It is usually measured in *decibels* (dB), and it is well known that these difference distortion metrics are not very well correlated with the human visible system (HVS). This might be a problem for their application in secret image sharing since sophisticated secret image sharing methods exploit in one way or the other effects of these schemes [22]. The detailed PSNR is represented by

$$\mathrm{PSNR} = 10 \times \log\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right), \tag{16}$$

where MAX indicates the maximum possible pixel value of the image. It is 255 because greyscale test images were used in this paper. MSE is the abbreviation for "*mean squared error*" and it is represented by

$$\mathrm{MSE} = \frac{1}{M^2} \sum_{i=0}^{M^2-1} \left(C_i - \mathrm{SH}_i\right)^2, \tag{17}$$

where M indicates the size of CI and SHI. C_i and SH_i are ith pixel values in CI and SHI, respectively. Given two greyscale images, if PSNR value is close to infinity (=∞), the distortion between two images is zero; that is, two images are the same. On the other hand, if PSNR value is close to zero, the distortion is higher; that is, two images are different. Generally, PSNR value is more than 35 dB, the difference between two images cannot be distinguished in HVS.

4.2. Analysis. In the experiments, we have performed the experiment for (3, 4)-threshold and used eight greyscale test images as shown in Figure 1. The sizes of CI and SHI were 512 × 512 and 512 × 512, respectively. And the size of SI was 256 × 256 or 512 × 512, depending on the experiments. The secret data was generated by Rand function in C++ Library. And then, generated secret bitstream was composed by each eight-bit. In order to implement the proposed scheme, the OpenCV Library and C++ programming language (environment: MS Visual Studio 2010) were used.

In the proposed scheme, PSNR result depends on the embedding method by prime p's interval as shown in Table 1. Our embedding method is that LSB1 and LSB2 were utilized. Hence, the minimum of PSNR without prime p is more than 44 dB because PSNR value of LSB2 embedding method is close to 44 dB in general. Depending on the change of prime p, PSNR result of the proposed scheme is shown in Table 2. If a prime p is 17, 19, or 29, PSNR values were higher than other values. This result was due to the embedding method in sharing phase. For example, maximum embedding capacity is 5-bit when the range of p is corresponding to $2^4 < p \le 2^5$. And, 5-bit is embedded into 3 pixels in CI by LSB1 and LSB2 (i.e., LSB1 − LSB2 − LSB2). On the other hand, if p is 11, the number of maximum embedding bits is four and it is embedded into 2 pixels in CI by LSB2. So, PSNR result was less than that of $16 < p \le 32$. Also, the number of maximum embedding bits is seven when p is 113. But PSNR values were less than that of range of $16 < p \le 32$ because LSB2 embedding technique was utilized once more (i.e., LSB1 − LSB2 − LSB2 − LSB2). In the experimental result of PSNR, the minimum was 44.11 dB. This result shows that we cannot distinguish the distortion between CI and SHIs in HVS.

In the meantime, we utilized a variable m in order to prevent the overflow and reinforce the security for secret data. So, the variable m and prime p should not be correlated relatively and Figure 2 shows that the relation of PSNR between p and m with prime p as 19 and 29. PSNR values were located at 45.10 to 45.60 dB regardless of the increase (or decrease) of m. This result shows that there is no correlation between p and m.

The embedding capacity of the proposed scheme was decided with the embedding method by prime p's interval as shown in Table 1. So, we have calculated the theoretical embedding capacity and it is shown in Table 3. MEBs, EC, t, and M indicate the number of maximum embedding bits, embedding capacity, threshold value, and size of shadow image, respectively. The embedding capacity is more increased when MEB is odd and p is close to 251. But, the embedding capacity is fixed at $2tM^2\lceil \log_2 m \rceil$ bit when MEB is even. This is because of the proposed embedding method as mentioned above. The best case is the intervals of $2^6 < p \le 2^7$ and $2^7 < p \le 2^8$ in terms of tradeoff between PSNR and the embedding capacity. And average of all embedding capacity values is $1.74tM^2\lceil \log_2 m \rceil$ bit.

In order to verify an excellence of the proposed scheme, we have performed a comparison between our and the previous schemes and the result of it is shown in Table 4. All results were average values and a unit of EC is bit-per-pixel (bpp). In EC results, the proposed and Lin and Chan's [18] schemes were related to a threshold value t. On the other hand, other

Table 2: PSNR result of (3, 4)-threshold proposed scheme by prime p.

p	SHI_1	SHI_2	SHI_3	SHI_4	Average
11	44.08	43.92	43.93	43.96	43.97
17	45.39	45.47	45.60	45.39	45.46
19	45.51	45.48	45.50	45.44	45.48
29	45.49	45.38	45.43	45.35	45.41
37	44.15	44.13	44.13	44.04	44.11
79	45.18	45.17	45.03	45.16	45.13
113	45.08	45.11	45.12	45.10	45.10
167	44.15	44.13	44.20	44.15	44.16
251	44.16	44.13	44.16	44.20	44.16

Table 3: The theoretical embedding capacity of the proposed scheme.

Interval	MEBs	EC (bit)
$2^0 < p \le 2^1$	1	$tM^2\lceil \log_2 m \rceil$
$2^1 < p \le 2^2$	2	$2tM^2\lceil \log_2 m \rceil$
$2^2 < p \le 2^3$	3	$\frac{3}{2}tM^2\lceil \log_2 m \rceil$
$2^3 < p \le 2^4$	4	$2tM^2\lceil \log_2 m \rceil$
$2^4 < p \le 2^5$	5	$\frac{5}{3}tM^2\lceil \log_2 m \rceil$
$2^5 < p \le 2^6$	6	$2tM^2\lceil \log_2 m \rceil$
$2^6 < p \le 2^7$	7	$\frac{7}{4}tM^2\lceil \log_2 m \rceil$
$2^7 < p \le 2^8$	8	$2tM^2\lceil \log_2 m \rceil$

Table 4: The comparison result between the proposed and previous schemes for the embedding capacity and PSNR.

Schemes	EC (bpp)	PSNR (dB)
Lin and Tsai [6]	1/2	39.17
Wang and Shyu [7]	1/4	—
Chang et al. [8]	3/4	40.92
Lin and Chan [22]	$(t-1)/3$	40.01
Proposed	$1.74t\lceil \log_2 m \rceil$	44.78

(a) Lena (b) Baboon (c) Airplane

(d) Peppers (e) Boat (f) Man

(g) Elaine (h) Woman

Figure 1: Eight greyscale test images.

schemes (Lin and Tsai [16], Wang and Shyu [23], and Chang et al. [24]) were fixed. This is because the amount of secret data that is inserted into polynomial is different. In typical schemes, the secret data is only embedded into the constant terms in the polynomial. But, the secret data is embedded into all coefficients except the highest order terms in Lin and Chan's scheme. If a threshold t is increased (this fact shows that the number of participants n is also increased), each EC is also increased more for our and Lin and Chan's schemes. But, EC and PSNR results in Lin and Chan's scheme have a inversely proportional relationship. In PSNR results, the proposed scheme was higher than others. We obtained that the efficiency and security of proposed scheme was superior to the previous schemes.

5. Conclusions

In this paper, we have proposed a (t, n)-threshold nonlinear secret image sharing scheme for the first time. Renvall and Ding's scheme was based on quadratic combination and Vandermonde matrix arithmetic operations. In the proposed scheme, it was extended to secret image sharing scheme with steganography concept. All arithmetic operations in the proposed scheme was limited within GF(251) because the

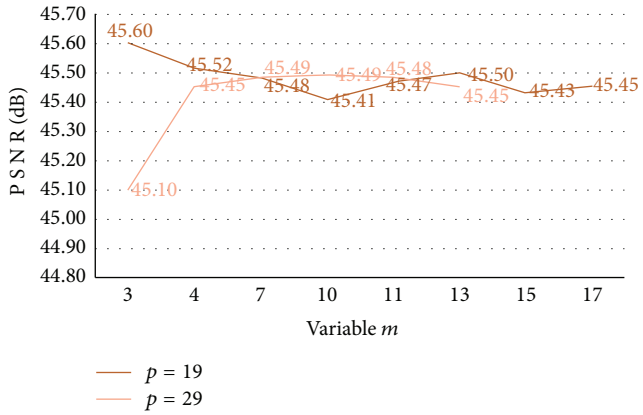

FIGURE 2: The relation of PSNR between p and m.

target of secret was a pixel value in SI. In order to prevent the overflow in SHI and reinforce the security, a new variable m was used in sharing procedure. In sharing procedure, the embedding technique depended on LSB1, LSB2, and prime p. XOR Boolean algebra operation for embedding data was performed in order to increase PSNR and the embedding capacity. As the results, the average values of PSNR and the embedding capacity are 44.78 (dB) and $1.74t\lceil \log_2 m \rceil$ (bpp), respectively. Also, the best case of the proposed scheme is the intervals of $2^6 < p \leq 2^7$ and $2^7 < p \leq 2^8$ in terms of tradeoff between PSNR and the embedding capacity.

The future works are as follows: the studies of nonlinear secret image sharing scheme over GF(2^n), the various experiments for PSNR and the embedding capacity, and the improved embedding technique.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2012R1A1A2008348) and Brain Korea 21 Plus (BK21+) Project in 2014.

References

[1] D. R. Stinson, *Cryptography Theory and Practice*, Chapman & Hall/CRC Press, 3rd edition, 2006.

[2] W. Stallings, *Cryptography and Network Security*, Prentice Hall, 4th edition, 2006.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the International Workshop on Managing Requirements Knowledge*, 1979.

[5] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.

[6] I. Mitsuru, S. Akira, and N. Takao, "Secret sharing scheme realizing general access structure," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 72, no. 9, pp. 1520–6440, 1989.

[7] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology—CRYPTO' 99*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 148–164, 1999.

[8] F. Paul, "A practical scheme for non-interactive verifiable secret sharing," in *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, pp. 427–438, 1987.

[9] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Advances in Cryptology—CRYPTO' 88*, vol. 403 of *Lecture Notes in Computer Science*, pp. 27–35, 1990.

[10] A. Beimel and B. Chor, "Secret sharing with public reconstruction," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1887–1896, 1998.

[11] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT'94*, vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, Springer, Berlin, Germany, 1995.

[12] M. Naor and A. Shamir, "Visual cryptography II. Improving the contrast via the cover base," in *Security protocols*, vol. 1189, pp. 197–202, Springer, Berlin, Germany, 1997.

[13] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the IEEE International Conference Image Processing (ICIP '94)*, vol. 2, pp. 86–90, Austin, Tex, USA, November 1994.

[14] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3-4, pp. 313–335, 1996.

[15] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[16] C. Lin and W. Tsai, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405–414, 2004.

[17] C. Thien and J. Lin, "An image sharing method with user-friendly shadow images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 12, pp. 1161–1169, 2003.

[18] P. Lin and C. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887–1893, 2010.

[19] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.

[20] C.-C. Chang and R.-J. Hwang, "Efficient cheater identification method for threshold schemes," *IEE Proceedings of Computers & Digital Techcuques*, vol. 144, no. 1, pp. 23–27, 1997.

[21] A. Renvall and C. Ding, "A nonlinear secret sharing scheme," in *Information Security and Privacy*, vol. 1172 of *Lecture Notes in Computer Science*, pp. 56–66, Springer, Berlin, Germany, 1996.

[22] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hidhing Techniques for Steganography and Digital Watermarking*, Artech House, London, UK, 2000.

[23] R.-Z. Wang and S.-J. Shyu, "Scalable secret image sharing," *Signal Processing: Image Communication*, vol. 22, no. 4, pp. 363–373, 2007.

[24] C. Chang, Y. Hsieh, and C. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.