User-Friendly Sharing System using Polynomials with Different Primes in Two Images

Hung P. Vo
Department of Engineering and Technology, Tra Vinh University,
No. 126 National Road 53, Tra Vinh City, Tra Vinh Province, Viet Nam

ABSTRACT
Yang *et al*. recently developed a user-friendly image-sharing scheme that shares images using many polynomials with different primes. Yang *et al*. modified the least significant bit (LSB) of original pixels to identify the prime number for sharing. However, the reconstructed image retains some noise. The scheme proposed in this work uses polynomials with different primes to generate pixel shadows without adjusting the LSBs of original pixels, such that the recovery process can reconstruct a high-quality original image using the Lagrange interpolation function.

Keywords
Image sharing, secret sharing, secret image sharing, user-friendly shadow image

1. INTRODUCTION
With the increasing need to share digital data through computer networks or telecommunications environments, the security of electronic data has become extremely important. A secret-sharing framework [1, 2] is a well-known cryptographic tool allowing users to share data. The first secret-sharing scheme was developed by Shamir in 1979 [1]. This framework, which was designed for use in a number system, requires adjustments for secret-image sharing. A previous secret-image-sharing scheme called a (*t, n*) threshold scheme [3, 4] allowed *n* participants to share secret images. Each participant has one part of the secret image called a shadow. For $2 \le t \le n$, where *t* and *n* are the threshold and number of shares, respectively. The secret image is encoded into *n* meaningless shadow images that are distributed to *n* participants. A secret image can be recovered if and only if any *t* or more than *n* shadow images with authorized participants are collected. Knowledge of any $(t-1)$ or fewer shadow images cannot be used to obtain a secret image. However, meaningless images transmitted over a public network attract attacker's attention. In 2003, Thien and Lin [5] designed an image-sharing method with user-friendly shadow images, each of which resembles a shrunken replica of the original image. In 2007, Yang *et al*. [6] identified problems in the scheme by Thien and Lin in that recovered pixel values may be outside the range of an 8-bit value in the decoding procedure when pixel values are close to 0 and 255 in an original gray-scale image. The framework by Yang *et al*. used polynomial functions with different prime numbers when encoding an original image (their scheme is discussed in Section 2). However, these two user-friendly image-sharing schemes use shadow images that contain a considerable amount of information from an original image, such that unauthorized users can apply image interpolation techniques to shadow images to acquire a high-quality original image. Furthermore, the quality of reconstructed images is always poor, such that they are not suitable for medical, military, or artistic applications [11, 12].

This work presents a novel user-friendly (2, 2) sharing scheme that encodes an original image *I* into two shadow images. The aim is to generate two user-friendly shadow images, each containing a small amount of information from the original image. This is essential to protect against access by unauthorized users while achieving high image quality after the original image is reconstructed.
The remainder of this paper is organized as follows. Section 2 briefly reviews related works. Section 3 presents the proposed scheme in detail. Experimental results are given in Section 4 and conclusions are presented in Section 5.

2. RELATED WORKS
In this section, two related works are introduced. First, Thien and Lin's user-friendly image-sharing scheme is described in Subsection 2.1. After that, Yang *et al.*'s user-friendly image sharing scheme with different primes is represented in Subsection 2.2.

2.1. The User-friendly Image-sharing Scheme by Thien and Lin
In Thien and Lin's (*t, n*) − threshold user-friendly image-sharing scheme [5], the original image is first divided into $t-$pixel non-overlapping blocks. Each block is classified as a smooth block or coarse block based on the following assumption: *t* pixels of the current block are $\{P_m, P_{m+1}, ..., P_{m+t-1}\}$, and $\tilde{P}_{m-1}$ is the decoded gray value of the last pixel in the previous block. Notably, $P_{\max}$ is the pixel in the current block (*i.e.*, $P_{\max} \in \{P_m, P_{m+1}, ..., P_{m+t-1}\}$), most different from $\tilde{P}_{m-1}$. The current block is a smooth block when $|P_{\max} - \tilde{P}_{m-1}| < 8$; otherwise, the block is a coarse block. For instance, in the (2, 4)–threshold system, a two-pixel (P_m, P_{m+1}) current block and the last pixel ($\tilde{P}_{m-1}$) in the previous block are (156, 158) and (155), respectively. As the expression $|158-155| > |156-155|$ is satisfied, $P_{\max}$ = 158. Hence, a two-pixel (156, 158) current block is a smooth block because the expression $|158-155| < 8$ holds. The sharing process is conducted via two formulas associated with the property of the block. For a smooth block, the sharing function is

$$S_k = (f_0 + f_1 \times k + f_2 \times k^2 + ... + f_{t-1} \times k^{t-1}) \bmod 17 \quad (1)$$

where $f_i = P_{m+i} - \tilde{P}_{m-1} + 8$ for $i = 0, 1, ..., t-1$. The shared pixels $\hat{P}_k$ are then evaluated by $\hat{P}_k = \tilde{P}_{m-1} + S_k - 8$ ($k = 1, 2, ..., n$). In a similar manner, the sharing function for the coarse block is:

$$E_k = (g_0 + g_1 \times k + g_2 \times k^2 + ... + g_{t-1} \times k^{t-1}) \bmod 17 \quad (2)$$

where $g_i = \left\lfloor \frac{P_{m+i}}{17} \right\rfloor$ for $i = 0, 1, \ldots, t-1$ and [.] is the rounding function. The n shared pixels are evaluated as follows:

$$\hat{P}_k = \begin{cases} P_{base} - E_k, & \text{if } P_{base} < \tilde{P}_{m-1}, \\ P_{base} + E_k, & \text{otherwise,} \end{cases} \quad (3)$$

where $P_{base} = \begin{cases} \lfloor P_{\max}/17 \rfloor \times 17, & \text{if } P_{\max} < \tilde{P}_{m-1} \\ \lceil P_{\max}/17 \rceil \times 17, & \text{otherwise} \end{cases}$

To illustrate this step using the above example, because (156, 158) is a smooth block, Eq. (1) is applied to encode the current block. A two-pixel current block with gray-scale values of (156, 158) combined with the previous pixel value of 155 will generate four values, $S_1 = 3$, $S_2 = 14$, $S_3 = 9$, and $S_4 = 2$, where $S_k = 9 + 11 \times k \bmod 17$, from which four shadow values, $\hat{P}_1 = 150, \hat{P}_2 = 161, \hat{P}_3 = 155,$ and $\hat{P}_4 = 149$ are produced, and ($\hat{P}_k = 155 + S_k - 8$).

However, some special cases will cause errors in a smooth image area and coarse area. Decoding a smooth block produces $P_{m+i} = \tilde{P}_{m-1} + f_i - 8$ because f_i is in the range of [0,16], and the value of (f_i − 8) is in the range of [-8,8]. Thus, when $\tilde{P}_{m-1}$ belongs to [0, 7] or [248, 255], the recovered values are $P_{m-i} \in$ [-8, -1] or [256, 263], respectively. These values are outside the conventional 8-bit image representation range. For the coarse block, when $P_{\max}$ = 255 in block (239, 255) and $P_{\max} \geq \tilde{P}_{m-1}$, P_{base} = $\lceil P_{\max}/17 \rceil \times 17 = 255$. Conversely, when $P_{\max} = 0$ in block (0, 16) and $P_{\max} \leq \tilde{P}_{m-1}$, $P_{\text{base}} = \lfloor P_{\max}/17 \rfloor \times 17 = 0$. Therefore, the shadow pixel results are $\hat{P}_k > 255$ and $\hat{P}_k < 0$. These drawbacks were noted by Yang *et al*. who developed another method, described briefly in next subsection, to solve these problems.

2.2. The User-friendly Image Sharing Scheme with Different Primes by Yang *et al*.

In Yang *et al.*'s (*t, n*) user-friendly image sharing scheme, the encoding phase first chooses a set of 2^t prime numbers. Assuming threshold is (2, *n*), the four prime numbers chosen must satisfy:

$$q_0 < q_1 < q_2 < q_3 \leq 251. \quad (4)$$

Next, the original image is divided into $t-$pixel non-overlapping blocks. With the threshold of $t = 2$, two pixels in the current block are denoted as (P_m, P_{m+1}) and two pixels in the previous block are denoted as (P_{m-2}, P_{m-1}). Notably, $P_{\max}$ is the pixel belonging to the current block $(P_{\max} \in \{P_m, P_{m+1}\})$ that differs most from P_{m-1}. In each two-pixel block, the least significant bits (LSBs) are modified as (00), (01), (10), or (11) to indicate prime numbers q_0, q_1, q_2, or q_3, respectively, and are used when encoding the next block. The LSBs in the previous block are modified as follows:

$$\begin{cases} LSB(P_{m-2}) = 0, LSB(P_{m-1}) = 0 \text{ for } |P_{\max} - P_{m-1}| \leq (q_0 - 1)/2 \\ LSB(P_{m-2}) = 0, LSB(P_{m-1}) = 1 \text{ for } (q_0 - 1)/2 < |P_{\max} - P_{m-1}| \leq (q_1 - 1)/2 \\ LSB(P_{m-2}) = 1, LSB(P_{m-1}) = 0 \text{ for } (q_1 - 1)/2 < |P_{\max} - P_{m-1}| \leq (q_2 - 1)/2 \\ LSB(P_{m-2}) = 1, LSB(P_{m-1}) = 1 \text{ for } (q_2 - 1)/2 < |P_{\max} - P_{m-1}| \leq 250 \end{cases}.$$

For instance, as two blocks, (P_{m-2}, P_{m-1}) and (P_m, P_{m+1}), equal (153, 155) and (157, 158), respectively, and four prime numbers, {q_0, q_1, q_2, q_3} equal {17, 61, 131, 251}, respectively, and |157 – 155| < |158 – 155|; thus, $P_{\max}$ = 158 and $|P_{\max} - P_{m-1}| < (q_0 - 1)/2$. Hence, the LSBs of pixels P_{m-2} and P_{m-1} are 0 (belonging to the first criterion in Eq. (5)). Consequently, pixel values P_{m-2} and P_{m-1} are 152 and 154, respectively. The *k*-th shadow for (P_m, P_{m+1}) is expressed as $S_k = (f_0 + k \times f_1) \bmod q_i$ (*i* = 0, 1, 2, 3) with f_0 and f_1 defined as:

$$\begin{cases} f_0 = (P_m - P_{m-1}) + (q_i - 1)/2 \\ f_1 = (P_{m+1} - P_{m-1}) + (q_i - 1)/2 \end{cases} \text{ for } i = 0, 1, 2, \quad (6)$$

$$\begin{cases} f_0 = \lfloor (P_m - P_{m-1})/2 \rfloor + (q_i - 1)/2 \\ f_1 = \lfloor (P_{m+1} - P_{m-1})/2 \rfloor + (q_i - 1)/2 \end{cases} \text{ for } i = 3. \quad (7)$$

The *n* shared pixels are evaluated using $\hat{P}_k \bmod q_i = S_k$ and the value $\hat{P}_k$ is close to the average value of pixels in the current block. For the same example, if S_k equals 11 for the current block (154, 156), then shared pixel $\hat{P}_k$ equals 147. Let {11, 28, 130, 147, 164, …, 249} be the set of numbers which satisfies the form 17 × *X* +11, where *X* is a non-negative integer. The pixel average value 155 (=(154+156)/2) is closest to the 147 in the set of numbers {11, 28, …, 130, 147, 164, …, 249}.

In this scheme, Yang *et al.* adjusted the LSB of each pixel in a block in the original image. This adjustment is for determining the appropriate prime number for the next block in the encoding phase. Because the values of pixels are changed, the quality of the recovered image is degraded. To overcome this shortcoming, this work proposes a user-friendly image -sharing scheme with a two-shadow framework based on multiple polynomials of different primes. The proposed scheme utilizes a location map to record prime number information instead of adjusting the LSBs of pixels. Therefore, reconstructed image quality is high.

3. THE PROPOSED SCHEME

This section describes the proposed user-friendly image-sharing scheme that uses two shadow images to achieve a high-quality image after reconstruction. The proposed scheme uses Shamir's polynomial function with different primes. Instead of changing the LSB value of pixels in the original image using the method used by Yang *et al*., the proposed scheme uses a location map containing prime number information for the encoding and decoding processes, which enhances the quality of a reconstructed image. Figure 1 shows the flowchart of the image-sharing scheme. The location map can be compressed using lossless compression methods, such as JBIG2 or the arithmetic coding toolkit, and the map can be used as the key shared by the sender and the receiver to enhance image security.

The proposed scheme has the following three phases. (1) The preprocessing phase truncates all gray-scale values in the range [251, 255] of the original image *I* to 250. This phase is also utilized to determine the prime number for each block, which is used to encode pixel blocks in the next phase. (2)

The sharing phase divides original image *I* into two shadow images using polynomials with different primes. (3) The recovery phase reconstructs the original image from two shadow images.

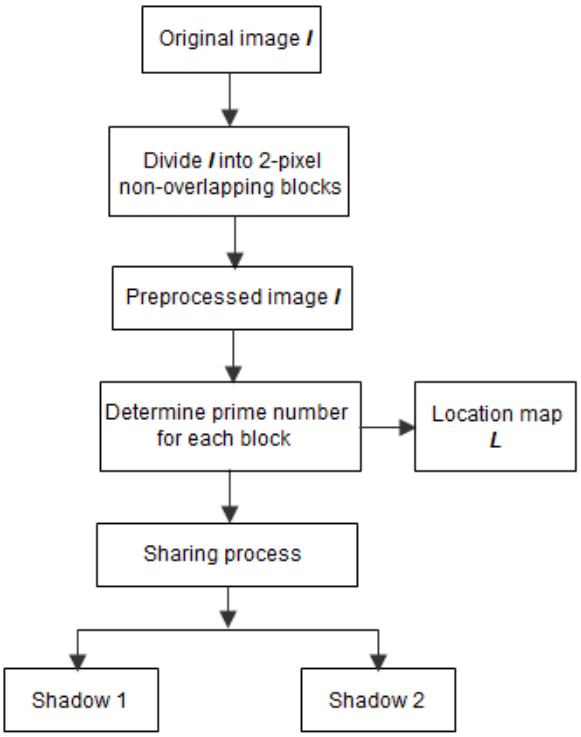

Figure 1. Flowchart of the sharing scheme

3.1 The Preprocessing Phase

As constrained by Eq. (4), the prime number used in the image-sharing polynomial function is not greater than 251, whereas the gray-scale value of a pixel is in the range of [0, 255]. Therefore, gray-scale values of original image *I* those are greater than 250 are truncated to 250. Next, the proposed framework initiates the sharing process by choosing a set of 2^2 prime numbers, namely, q_0, q_1, q_2, and q_3, which are constrained by $q_0 < q_1 < q_2 < q_3$ and $q_3 \le 251$. Original image *I* is then divided into 2-pixel non-overlapping blocks and the initial location map is set at $L = 0$. For each two pixels in the block, the indicators assigned are 0 and 0, 0 and 1, or 1 and 0 for id_1 and id_2 to indicate prime numbers q_0, q_1, or q_2, respectively. For the block encoded by prime number q_3, the location map is set to 1 at the position corresponding to the current block. Suppose the gray-scale values of pixels in the current block in the preprocessed image are (P_m, P_{m+1}) and the gray-scale value of the second pixel in the previous block is P_{m-1}. If the current block is the initial block (no previous block exists), P_{m-1} is set to 0. The prime number of the current block is derived as follows:

$$\begin{cases} id_1 = 0, id_2 = 0, prime = q_0 & \text{for } |P_{\max} - P_{m-1}| \le (q_0 - 1)/2, \\ id_1 = 0, id_2 = 1, prime = q_1 & \text{for } (q_0 - 1)/2 < |P_{\max} - P_{m-1}| \le (q_1 - 1)/2, \\ id_1 = 1, id_2, = 0, prime = q_2 & \text{for } (q_1 - 1)/2 < |P_{\max} - P_{m-1}| \le (q_2 - 1)/2, \\ L_j = 1, \quad prime = q_3 & \text{for } (q_2 - 1)/2 < |P_{\max} - P_{m-1}| \le 255, \end{cases} \quad (8)$$

where $P_{\max} = \begin{cases} P_m, & \text{if } |P_m - P_{m-1}| > |P_{m+1} - P_{m-1}| \\ P_{m+1}, & \text{otherwise} \end{cases}$

3.2 The Sharing Phase

After the preprocessing phase, each block is assigned a prime number, which is utilized to compute coefficients f_0 and f_1 for the polynomial function as follows:

$$\begin{cases} f_0 = P_m - P_{m-1} + (q_i - 1)/2 \\ f_1 = P_{m+1} - P_{m-1} + (q_i - 1)/2 \end{cases} \quad \text{for } i = 0, 1, 2, \quad (9)$$

$$\begin{cases} f_0 = \lfloor (P_m - P_{m-1})/2 \rfloor + (q_i - 1)/2 \\ f_1 = \lfloor (P_{m+1} - P_{m-1})/2 \rfloor + (q_i - 1)/2 \end{cases} \quad \text{for } i = 3 \quad (10)$$

where $\lfloor x \rfloor$ is the floor function that is the largest integer not greater than x.

Both f_0 and f_1 are used as coefficients for the following polynomial in a way similar to that in Eq. (1):

$$S_k = (f_0 + k \times f_1) \bmod q_i \quad \text{for } i = 0, 1, 2, \text{and } 3 \quad (11)$$

The two output values, S_1 and S_2, are applied to evaluate shared pixels $\hat{P}_k$.

To achieve user-friendly image sharing, shared pixels $\hat{P}_k$ are then computed by associating output values S_k with the current block in the original image. The value $\hat{P}_k$ is evaluated as follows:

Case 1: The prime number is q_0, q_1, or q_2

$\hat{P}_k$ is closest to the average pixel value and satisfies the following two constraints:

(1) $\hat{P}_k \bmod q_i = S_k$, ($i$ = 0, 1, 2).

(2) LSB($\hat{P}_k$) = id_k, LSB(.) is the function obtaining the LSB.

Case 2: The prime number is q_3

$\hat{P}_k = S_k$.

Shared pixels $\hat{P}_k$ are sequentially assigned to the two shadow images. Because each block has two pixels of the secret image, each shadow image receives only one of the two generated pixels. The size of each shadow image is half that of the secret image.

An example is utilized to illustrate this phase. Assume after the preprocessing phase, given pixels $P_{m-1} = 156$, $P_m = 157$, and $P_{m+1} = 158$ with four prime numbers are chosen as $q_0 = 17$, $q_1 = 61$, $q_2 = 127$ and $q_3 = 251$.

Because $|P_{m+1} - P_{m-1}|$ is larger than $|P_m - P_{m-1}|$, $P_{\max} = 158$. Additionally, $|P_{\max} - P_{m-1}|$ satisfies the first criterion in Eq. (8). Therefore, $id_1 = 0, id_2 = 0$, and $pime = q_0 = 17$. Since the current block is encoded with q_0=17, depending on Eq. (9), f_0 and f_1 are 9 and 10, respectively.

Using f_0 and f_1 as coefficients to construct the polynomial function and Eq. (11), two output values, $S_1 = 2$ and $S_2 = 12$ are generated. Notably, $S_1 = 2$ when the average value of the current block (157, 158) equals 157; thus, $\hat{P}_1$ = 172. The reason is that the selected value of 172 is closest to the average pixel value of the current block and satisfies two constraints. They are: (1) 172 mod 17 = S_1= 2, and (2) LSB(172) = $id_1 = 0$. In a similar way, $S_2 = 12$ and the

average value equals157; thus, $\hat{P}_1$ = 148, because 148 is closest to the average pixel value and satisfies two constraints, (1) 148 mod 17 = S_1= 12, and (2) LSB(148) = $id_1 = 0$.

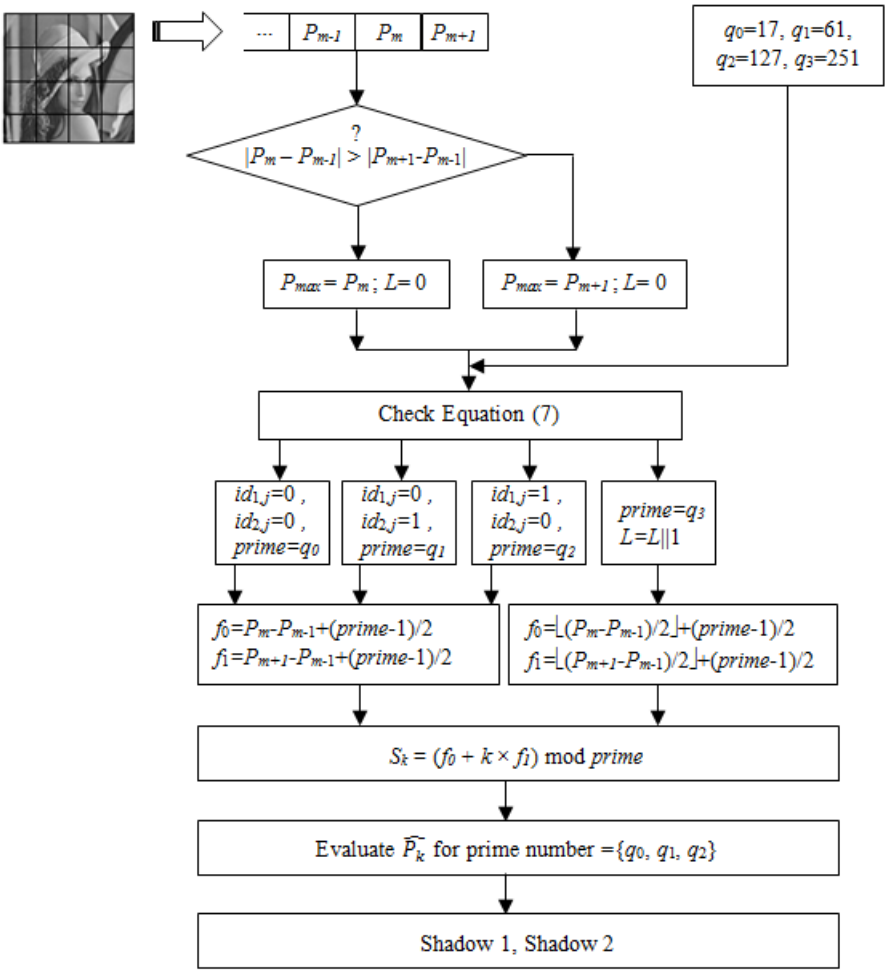

Figure 2. An example of the proposed scheme

3.3 The Recovery Phase

The process for revealing a reconstructed image starts by determining the prime number from shadow pixels and the location map. If the location map corresponds to the block that will be recovered is 1, then the prime number is q_3; otherwise, the prime number is determined depending on the LSBs of shadow pixels. The revealing process has the following steps.

Step 1: Take the first pixel from each of the two shadow images, S_1 and S_2.

Step 2: Identify the prime number. If L = 1, the prime number is q_3; otherwise, the prime number is determined using the LSBs of two shadow pixels, such as (00), (01), or (10), to obtain prime numbers of q_0, q_1, or q_2.

Step 3: Apply Lagrange interpolation to generate coefficients f_0 and f_1.

Step 4: Apply Eq. (9) or Eq. (10) depending on the prime number to recover pixels P_m and P_{m+1} from the original block.

Step 5: Repeat Steps 1 to 4 by taking the next pixel in each two shadow images until all pixels are processed.

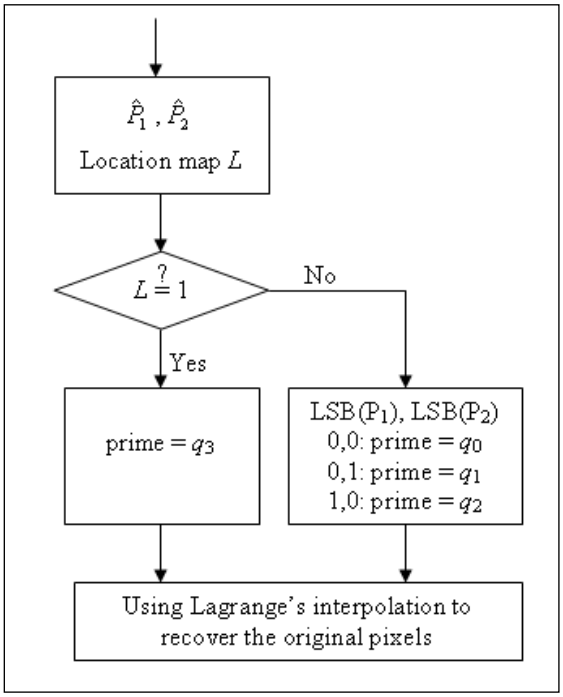

Figure 3. Flowchart of the reveal phase

4. EXPERIMENTAL RESULTS

Figure 4 shows experimental results from applying the proposed user-friendly image-sharing scheme with different prime numbers. Here Lena is the input image. Figure 4(a) shows the original image sized 512×512. Figures 4(b) to 4(c) show the two shadow images, each half of the original image in size. Each shadow image resembles a portrait of the original image. This similarity allows users to recognize each shadow image without any computations, thereby providing a user-friendly interface for identifying shadow images with the naked eye. However, important information is omitted from this view. Figure 4(f) shows the image reconstructed using the proposed method that has higher quality than images reconstructed with other methods [5, 6, 10] (Table 1). The quality of the reconstructed image is analyzed using the peak signal-to-noise ratio (*PSNR*). The *PSNR* is derived as

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (12)$$

The mean square error (*MSE*) is derived as

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{i,j} - p'_{i,j})^2 \quad (13)$$

where $m \times n$ is the size of an image, $p_{i,j}$ is the original pixel value, and $p'_{i,j}$ is the reconstructed image.

(a) (b) (c)

(d) (e)

(f)

Figure 3. Experimental results obtained with the proposed scheme with the prime numbers $\{q_0, q_1, q_2, q_3\}$ = {17, 61, 131, 251} using Lena image

(a) Original image size is 512×512;
(b) and (c) are two shadow images;
(d) and (e) are two expanded images from (b) and (c) respectively;
(f) Recovered image using shadow images (b) and (c).

Table 1 shows the *PSNR*s of the expanded images and recovered image by the proposed scheme and other schemes. The *PSNR* indicate that the reconstructed image by the proposed scheme has higher quality than those by other schemes (last column in Table 1). The *PSNR*s of the expanded images and the original image by the proposed method are slightly lower than those of images reconstructed using other methods. Notably, one of the most important goals of the proposed user-friendly image-sharing scheme is to provide distinguishable content among numerous shadow images. However, if a shadow image has too much information from the original image, unauthorized users may obtain a shadow image and route it using image interpolation techniques to acquire a high-quality image. Thus, the ability to preserve the original image content may be eliminated in such a system.

Table 1. Image qualities by different image-sharing schemes using Lena image

	The expanded image	**The recovered image**
Thien and Lin [5]	24.59	39.93
Yang et al. [6]	23.32	50.53
Wang et al. [10]	19.13	51.13
Proposed scheme	18.80	58.10

5. CONCLUSION

The paper has proposed a user-friendly image-sharing system using polynomials with different primes. In this user-friendly image-sharing scheme, shadow images resemble shrunken versions of an original image. Although the number of shadow images is limited to 2 in the proposed method, it can reconstruct a high-quality original image. Moreover, it provides user-friendly shadow images to receivers who can then recognize the image. However, receivers do not know the content of an image exactly when those involved do not cooperate. Based on the *PSNR* values, experimental results confirm that the proposed scheme generates high reconstructed image quality.

6. REFERENCES

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

[2] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of AFIPS 1979 National Computer Conference*, Vol. 48, pp. 313–317, 1979.

[3] C. C. Thien and J. C. Lin, " Secret image sharing," *Computers and Graphics*, Vol. 26, pp. 765–770, 2002.

[4] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptography: Eurocrypt'94*, pp. 1–12, 1995.

[5] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, pp. 1161–1169, 2003.

[6] C. N. Yang, K. H. Yu, and R. Lukac, "User-friendly image sharing using polynomials with different primes," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 17, pp. 40–47, 2007.

[7] C. C. Chang, C. C. Lin, C. H. Lin, and Y. H. Chen, " A novel secret image sharing scheme in color images using small shadow images," *Information Sciences*, Vol. 178, pp. 2433–2447, 2008.

[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] P. Y. Lin and C. S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, Vol. 31, Vol. 31, pp. 1887-1893, 2010.

[10] R. Z. Wang, Y. F. Chien, and Y. Y. Lin, " Scalable user-friendly image sharing," *Journal of Visual Communication and Image Representation*, Vol. 21, pp. 751-761, 2010.

[11] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 18, pp. 497–509, 2008.

[12] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, pp.890–896, 2003.