Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

Novel Lossless Morphing Algorithm for Secret Sharing via Meaningful Images

Qian Mao

School of Optical-Electrical and Computer Engineering
University of Shanghai for Science and Technology
No. 516, Jungong Rd., Yangpu, Shanghai, 200093, P. R. China
maoqiansh@gmail.com

K. Bharanitharan

Research School of Management
The Australian National University, ACT, Australia
dharan@ieee.org

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wenhwa Rd., Seatwen, Taichung, 40724, Taiwan
alan3c@gmail.com

Received April, 2016; revised July, 2016

Abstract. *Image morphing algorithms create an intermediate image that resembles both the source image and the target image simultaneously. Most existing morphing algorithms incur information loss, thus, they cannot reconstruct the original images accurately. This paper proposes a novel, lossless image morphing (LIM) algorithm, designed so that the original image can be losslessly reconstructed from the morphed image. Additionally, the proposed LIM algorithm is used for secret image sharing in which the shares are generated by the image morphing operation. The shares are high-quality, natural images, and the secret image can be losslessly reconstructed, under the condition that all of the shareholders work cooperatively. Due to non-linear warping in the LIM algorithm, the proposed secret image sharing scheme is unconditionally secure.*
Keywords: Secret image sharing; Image morphing; Meaningful share; Lossless reconstruction.

1. **Introduction.** A (t, n)-threshold secret image sharing (SIS) scheme divides a secret image into n shares in such a way that the secret image can be reconstructed by the cooperation of any t or more than t shareholders, and there is a strict rule that fewer than t shares cannot cooperatively reconstruct the secret image.

There are two categories in the area of SIS in the current literature, i.e., visual secret sharing (VSS) and computation-based secret image sharing (CBSIS). VSS also is called visual cryptography, which was first introduced by Naor and Shamir [1]. In their scheme, each pixel in the original secret image is divided into several shares, and each share contains q sub-pixels. The reconstruction of the secret image is achieved by overlapping the shares, which allows the secret image to emerge. Naor *et al.*'s scheme enlarged the size of the share by a factor of q. To diminish the share size, Yang proposed a VSS scheme that uses a probabilistic method that has no expansion of the shares [2]. Using an integer

linear program, Shyu and Chen proposed a model that minimizes the pixel expansion of the VSS [3]. To solve the problem of reconstruction failure due to the dislocation of the shares, Wang *et al.* proposed a $(2, n)$ VSS scheme that allows shares' shift to a certain extent in the reconstruction process [4]. Recently, the VSS schemes based on random grids have attracted a lot of attention, because they cause no pixel expansion and provide better quality to the reconstructed images [5, 6, 7]. In 2012, Iwamoto proposed a notion of weak security of the VSS scheme and pointed that most of the VSS schemes are visually secure instead of unconditionally secure. Furthermore, they proposed two weakly secure VSS schemes for color images [8]. By adding a cover image to each share, Lee and Chiu proposed a visual cryptography algorithm of which shares are meaningful images [9]. Using visual information pixel synchronization and error diffusion, Kang *et al.* proposed a visual cryptography scheme that shares the secret via meaningful color shares [10].

Most of the VSS schemes reconstruct the secret image with low quality, because a lot of information was lost during the secret sharing process. To increase the quality of the reconstructed image, secret image sharing schemes with computational reconstruction attracted a great deal of attention; such schemes are referred to as computation-based secret image sharing schemes in this paper. Many existing CBSIS schemes share the secret image using Shamir's secret sharing scheme [11], but the shares generated by this approach are noise-like, which tend to arouse attacker's attention [12, 13]. To solve this problem, Lin *et al.* proposed a meaningful SIS scheme, which uses steganography to embed the noise-like shares into cover images [14]. Considering the information loss caused by noise in transmission or storage, Chang *et al.* proposed a meaningful SIS scheme that has the ability to remedy this problem by detecting and repairing the corrupted area in the secret image [15]. Aarti *et al.* proposed a (t, n)-threshold CBSIS scheme, which divides the bit plane images of the secret image by the traditional binary secret sharing scheme, then, it hides the shares in stego images as watermarks [16]. Lee *et al.* proposed a SIS scheme that shares a secret image by $n - 1$ natural images and one noise-like image [17].

For most lossless, meaningful CBSIS schemes, the secret image is hidden in several meaningful cover images as a watermark, which actually can be regarded as an application of steganography. In this paper, a novel CBSIS scheme based on the image morphing technique is proposed for the first time. Image morphing is currently used extensively in cinematic special effects, which creates a morphed image with a source image and a target image. The morphed image resembles the source and target images simultaneously. There are several kinds of morphing algorithms, such as Wolberg's skeleton-based morphing algorithm [18], Beier and Neely's feature-based morphing algorithm [19], Zhu's optimal-mass-transport-based algorithm [20], and Lin's patch-based algorithm [21]. Recently, image morphing algorithms for three-dimensional images have attracted extensive attention [22, 23, 24, 25]. Most researches in the area of image morphing focus on how to create a morphed image with high visual quality. In this paper, we propose a novel image morphing algorithm in which we focus on the reconstruction of the original image from the morphed image. The main contributions of our work include:

1. All of the existing image morphing algorithms lead to information loss, i.e., some pixels in the source image and the target image are lost in the morphing operation. In this paper, a lossless image morphing (LIM) algorithm was proposed for the first time, for which the original image (either source image or target image) can be losslessly reconstructed from the morphed image.
2. A sequential morphing algorithm, which integrates several images into one image after morphing, was proposed for the first time.

3. An SIS scheme based on LIM was proposed, offering the advantages of (a) the shares are meaningful images with relatively high quality and (b) the reconstructed image is identical to the original secret image.

The rest of the paper is organized as follows. Section 2 briefly introduces the conventional image morphing algorithm. Section 3 describes our proposed lossless image morphing and de-morphing algorithm. Our secret image sharing schemes based on LIM are proposed in Section 4. In Section 5, the performance comparisons with the existing CBSIS schemes and the security analyses of the proposed schemes are presented. Our conclusions are presented in Section 6.

2. **Brief Introduction to Image Morphing.** The aim of image morphing is to create a middle image between a source image and a target image in such a way that the morphed image simultaneously has the features of the two images. Assume that the original source image is I_S^o and the original target image is I_T^o, both of which have a size of $M \times N$. The morphing algorithm first selects r control points in the source image. The coordinates of the control points in the source image are recorded as $C_S = \begin{bmatrix} x_1^S & x_2^S & \cdots & x_r^S \\ y_1^S & y_2^S & \cdots & y_r^S \end{bmatrix}^T$, where (x_i^S, y_i^S) are the coordinates of the i^{th} control point ($i \in [1, r]$). After that, r control points are selected from the target image, the coordinates of which are $C_T = \begin{bmatrix} x_1^T & x_2^T & \cdots & x_r^T \\ y_1^T & y_2^T & \cdots & y_r^T \end{bmatrix}^T$. It should be noted that the locations of the control points in the source and target images should correspond one-to-one with respect to the characteristics of the images. A scheme to automatically select the control points for image morphing was proposed in our previous work [26].

According to C_S and C_T, a difference matrix, C_d, can be obtained, i.e., $C_d = C_T - C_S = \begin{bmatrix} c_1^h & c_2^h & \cdots & c_r^h \\ c_1^v & c_2^v & \cdots & c_r^v \end{bmatrix}^T$, where $c_i^h = x_i^T - x_i^S$ and $c_i^v = y_i^T - y_i^S (i \in [1, r])$. Each column of matrix C_d represents the distances (horizontal and vertical, respectively) between the control points in the source image and their corresponding control points in the target image. Following that step, two linear interpolations are implemented to the two columns of C_d independently. To achieve the interpolation value, first, the coordinates of the control points in the source (or target) image are attached to the elements of C_d, i.e., $C_d = \begin{bmatrix} c_1^h(x_1^S, y_1^S) & c_2^h(x_2^S, y_2^S) & \cdots & c_r^h(x_r^S, y_r^S) \\ c_1^v(x_1^S, y_1^S) & c_2^v(x_2^S, y_2^S) & \cdots & c_r^v(x_r^S, y_r^S) \end{bmatrix}^T$. Then, the first column of C_d is taken and all of the elements are put into a three-dimensional space, for which x_i^S, y_i^S, and c_i^h act as the x-value, y-value, and z-value, respectively ($i \in [1, r]$). After that, we use all of these points to segment the xy-plane in such a manner that every partition is a quadrilateral and all of the quadrilaterals do not overlap. Then, for a quadrilateral $[(x_i^S, y_i^S), (x_j^S, y_j^S), (x_k^S, y_k^S), (x_l^S, y_l^S)](i, j, k, l \in [1, r]$ and $i \neq j \neq k \neq l)$, the z-value, p^h, of an arbitrary point, (x, y), within the quadrilateral can be obtained by the following linear interpolation function:

$$
\begin{aligned}
p^h(x,y) &= \frac{y_u - y}{y_u - y_d} p_d + \frac{y - y_d}{y_u - y_d} p_u, \\
y_d &= \frac{x_l^S - x}{x_l^S - x_i^S} \cdot y_i^S + \frac{x - x_i^S}{x_l^S - x_i^S} \cdot y_l^S, y_u = \frac{x_k^S - x}{x_k^S - x_j^S} \cdot y_j^S + \frac{x - x_j^S}{x_k^S - x_j^S} \cdot y_k^S, \\
p_d &= \frac{x_l^S - x}{x_l^S - x_i^S} \cdot c_i^h + \frac{x - x_i^S}{x_l^S - x_i^S} \cdot c_l^h, p_u = \frac{x_k^S - x}{x_k^S - x_j^S} \cdot c_j^h + \frac{x - x_j^S}{x_k^S - x_j^S} \cdot c_k^h.
\end{aligned} \tag{1}
$$

This linear interpolation is implemented in the range of $M \times N$ of the xy-plane. The same operation is implemented to the second column of C_d. Then, two interpolation matrices, $p^h = \{p^h(x,y)|x \in [1,M], y \in [1,N]\}$ and $p^v = \{p^v(x,y)|x \in [1,M], y \in [1,N]\}$, can be obtained. The elements, $p^h(x,y)$ and $p^v(x,y)$, in the interpolation matrices indicate the horizontal and vertical distances between the pixel $I_S^o(x,y)$ in the source image and its corresponding pixel in the target image.

After that, a morphing rate, α, is selected in the range of $[0,1]$. The value of the morphing rate determines how much the morphed image resembles the source and target images. The larger the morphing rate, the more the morphed image resembles the target image. According to P^h, P^v, and α, both the source image and the target image are warped by shifting their pixels. For the source image, the horizontal and vertical distances, D_S^h and D_S^v, between the pixels' original locations and their locations in the warped image are:

$$D_S^h = [\alpha P^h], D_S^v = [\alpha P^v]. \tag{2}$$

where $[X]$ represents to round all of the elements in matrix X. For the target image, the horizontal and vertical distances, D_T^h and D_T^v, between pixels' original locations and their locations in the warped image are:

$$D_T^h = [(1-\alpha)P^h], D_T^v = [(1-\alpha)P^v]. \tag{3}$$

According to the shifting distances, both the source image and the target image are warped, and two warped images, I_S^w and I_T^w, are obtained as follows:

$$I_X^w(i,j) = I_X^o(i + D_X^h(i,j), j + D_X^v(i,j)), \tag{4}$$

where X represents S or T, $i \in [1,M]$, and $j \in [1,N]$.

The morphed image, I_{ST}^m, is obtained by adding the two warped images, i.e.:

$$I_{ST}^m = (1-\alpha)I_S^w + \alpha I_T^w. \tag{5}$$

3. **Proposed Lossless Image Morphing Algorithm.** Most of the existing morphing algorithms lead to information loss. In this section, the reason for pixel loss is analyzed in Subsection 3.1. On this basis, the novel, lossless image morphing algorithm is proposed in Subsection 3.2. Considering the special applications of image morphing in the SIS scheme proposed in Section 4, the method of selecting the control points for the LIM is proposed in Subsection 3.3.

3.1. **Analysis of pixel loss in conventional image morphing.** For the image morphing algorithm based on conventional mesh warping, the mesh is non-uniform, and there are overlaps during the warping process. The phenomenon of overlap occurs under the following condition:

$$[i_1 + D_X^h(i_1,j_1), j_1 + D_X^v(i_1,j_1)] = [i_2 + D_X^h(i_2,j_2), j_2 + D_X^v(i_2,j_2)], \text{if } i_1 \neq i_2 \text{ or } j_1 \neq j_2, \tag{6}$$

where X represents S or T, $i_1, i_2 \in [1,M]$, and $j_1, j_2 \in [1,N]$.

Thus, during the warping process shown in (4), the mapping relationships between the pixels' original positions and their new positions in the warped image do not correspond one-to-one. Some pixels in the original image may be mapped into more than one position in the warped image, while some pixels may not be mapped into any position in the warped image, which leads to information loss. Figure 1 shows an example of pixel loss, in which a black and white image is warped and each number-labeled block represents a pixel. Image (a) is the original image with a black circle in it. Image (b) is the warped image in which the circle is warped to an ellipse. During this warping process, some pixels in the original image are transferred to two positions in the warped image, such as pixels

17, 18, 19, 31, 32, and 33, and some pixels in the original image are not transferred to any position in the warped image, such as the red-marked pixels 4, 10, 12, 38, 40, and 46. The pixels that were not mapped into the warped image are lost.

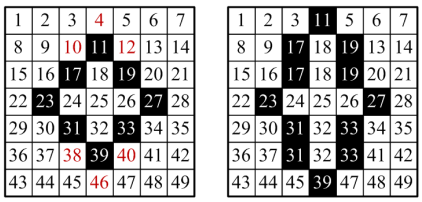


FIGURE 1. Conventional mesh warping (a) original image (b) warped image

3.2. **Lossless image morphing and de-morphing.** In the following, a novel, lossless, mesh warping algorithm is proposed, which maps all of the pixels in the original images into the warped image. To obtain this goal, the distances of the pixels between their original positions and their warped positions for the source image, D_S^h and D_S^v, and those for the target image, D_T^h and D_T^v, are computed by (2) and (3) for the first step. After that, both the source image and the target images are preliminarily warped as follows:

$$I_X^w(i + D_X^h(i,j), j + D_X^v(i,j)) = I_X^o(i,j), \tag{7}$$

where X represents S or T, $i \in [1, M]$, and $j \in [1, N]$. Comparing (7) with (4), we find that the conventional mesh warping function provides a gray value for every position in the warped image, but it does not guarantee that all of the pixels in the original image are mapped into the warped image. On the contrary, our mesh warping function makes sure that all of the pixels in the original image are mapped into the warped image. But, in so doing, some pixels may be transferred to the same position in the warped image, and these are defined as colliding pixels. Figure 2 shows an example of the proposed warping algorithm. In order to pinpoint the pixels, a two-dimensional coordinate plane is added to each image. In this example, the original image, Figure 2(a), is the same as Figure 1(a). The preliminarily warped image obtained by (7) is shown in Figure 2(b), in which the blocks with two numbers represent the colliding circumstances and the gray blocks denote the blank locations. Considering the location (1, 4) in Figure 2(b) as an example, the original pixels with numbers 4 and 11 are collided in this location, thus, only one pixel can be recorded and the other one is erased. On the other hand, some locations, such as location (3, 3) in Figure 2(b), are blank because there is no pixel in the original image transferred to these positions.

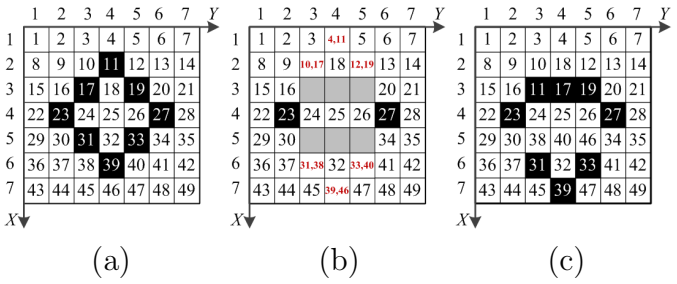


FIGURE 2. Proposed mesh warping (a) original image (b) preliminary warped image (c) final warped image

Since the original image and the warped image have the same size, the amount of the lost pixels must be identical to the amount of the blank locations in the preliminary warped image. Thus, we select a blank location for each lost pixel and transfer the lost pixel to the blank location. For example, since two pixels collide in location (1, 4) in Figure 2(b), the pixel with number 4 (or 11) is remained in this location and the pixel with number 11 (or 4) is transferred to a blank location (3, 3). By this approach, a one-to-one relationship between all of the lost pixels and all of the blank locations can be built. It should be noted that this relationship can be arbitrarily determined, but it must be consistent in both morphing and de-morphing algorithms. The final warped image using this method is shown in Figure 2(c).

By this approach, the proposed warping algorithm generates a one-to-one relationship between every pixel in the original image and every location in the warped image, thus, no information is lost during the warping operation. For the pixel (i, j) in the original image, its destination location in the warped image, $(W_X^h(i,j), W_X^v(i,j))$, can be denoted as:

$$\begin{aligned} &W_X^h(i,j) = i + D_X^h(i,j), W_X^v(i,j) = j + D_X^v(i,j), \\ &\text{where}(W_X^h(i_1,j_1), W_X^v(i_1,j_1)) \neq (W_X^h(i_2,j_2), W_X^v(i_2,j_2)), \text{if}(i_1,j_1) \neq (i_2,j_2), \end{aligned} \tag{8}$$

where X represents S or T, $i, i_1, i_2 \in [1, M]$, and $j, j_1, j_2 \in [1, N]$.

According to the meshes, both the source image and the target image finally are warped as follows:

$$I_X^{nw}(W_X^h(i,j), W_X^v(i,j)) = I_X^o(i,j), \tag{9}$$

where X represents S or T. Using (9), two lossless warped images, I_S^{nw} and I_T^{nw}, are obtained. Substituting I_S^{nw} and I_T^{nw} into (5), the losslessly morphed image can be created. The lossless image morphing algorithm can be represented as follows:

$$I^m = \text{LM}(I_S^o, I_T^o, C_S, C_T, \alpha), \tag{10}$$

where LM is the lossless morphing function.

For the proposed LIM algorithm, the original source/target image can be losslessly reconstructed using the morphed image, the target/source image, the control points, and the morphing rate. Without loss of generality, we present the reconstruction of the target image. To reconstruct the target image from the morphed image, first, the de-morphing algorithm warps the source image using (9) and obtains a same warped source image, I_S^{nw}, as that in the morphing algorithm. After that, the warped target image can be computed as follows:

$$I_T^{nw} = \frac{I^m - (1-\alpha) I_S^{nw}}{\alpha}. \tag{11}$$

To restore the target image, all of the shifted pixels in the warped image, I_T^{nw}, should be shifted back to their original positions. Thus, the non-overlapped meshes for the target image, W_T^h and W_T^v, are created by C_S, C_T, α using (8). Note that since the morphing parameters are the same for both the morphing algorithm and the de-morphing algorithm, the same meshes can be obtained by both sides. Thus, according to W_T^h and W_T^v, all the pixels in I_T^{nw} can be shifted back to their original positions by the following function:

$$I_T^r(i,j) = I_T^{nw}(W_T^h(i,j), W_T^v(i,j)), \tag{12}$$

where $i \in [1, M]$ and $j \in [1, N]$. The reconstructed target image, I_T^r, is identical to the original target image, I_T^o. By this approach, our proposed scheme completely reconstructs the original image. The lossless de-morphing algorithm can be summarized as follows:

$$I_T^r = \text{LD}(I^m, I_S^o, C_S, C_T, \alpha), \tag{13}$$

where LD is the lossless de-morphing function.

In the following, the results of the morphing experiments using the proposed LIM and LDM algorithms are presented. The experimental results are shown in Figure 3, where (a) is the source image, and (b) is the target image on which the control points are marked with crosses. Images (c), (d), and (e) are the morphed images with the morphing rates of 0.1, 0.5, and 0.9, respectively. Image (f) is the reconstructed target image, which is completely the same as (b).

(a) (b) (c) (d) (e) (f)

FIGURE 3. Experimental results (a) source image (b) target image (c) morphed image ($\alpha = 0.1$) (d) morphed image ($\alpha = 0.5$) (e) morphed image ($\alpha = 0.9$) (f) reconstructed target image

The experimental results indicated that the morphed image that had a small morphing rate (Figure 3(c)) resembled the source image, and it was almost impossible to recognize the features of the target image from it. We defined the range of the morphing rate, $\alpha < \alpha_s$, as the *source range*. On the contrary, when the morphing rate was large enough (Figure 3(e)), the morphed image resembled the *target image*, and we could not discern the source image from it. We defined the range of the morphing rate, $\alpha > \alpha_t$, as the *target range*. The morphing range, $\alpha_s < \alpha < \alpha_t$, was defined as the *middle range*.

There are two problems in the morphed image, i.e., *ghost shadow* and *relocation noise*, as shown in Figures 3(c), (d), and (e). Ghost shadows are the overlapped, blurred figures appeared in the morphed images, which are caused by the overlay of two different images. Since the source and the target images are not completely the same even after image warping, the ghost shadows cannot be avoided entirely. Relocation noise is the discontinuous lines and points in the morphed image. In the warping phase, some collided pixels are relocated to the blank locations. The pixels transferred to the blank positions have no correlations with their neighboring pixels, so discontinuities occur in the morphed image, which are relocation noise. When the morphed image belongs to the source/target range, the source/target image will cover the target/source image to a large extent, so both the ghost shadows and the relocation noise are insignificant.

3.3. **Selection of control points.** The goal of the conventional image morphing is to create natural images. The more natural the morphing image is, the more highly the morphing algorithm is evaluated. To diminish the ghost shadows, two requirements must be satisfied, i.e.:

1. The source and target images must have similar features. For example, both of them are human faces.
2. The control points in the source and target images should correspond one-to-one. For example, the pixels on the tip of the nose in the source and the target images, respectively, can be selected as a pair of corresponding control points.

Inappropriate selection of the control points will lead to severe ghost shadows, thus, in conventional image morphing operations, control points must be sophisticated selected. However, in our secret image sharing scheme proposed in the following section, the goal

of image morphing is to hide the target image in the source image, which means that the morphed image should belong to the source range. Since the features of the source image will cover the features of the target image in this situation, there is no need to strictly consider the corresponding relationship of the control points in the two images, and the two images with different structures and features can even be morphed together, as shown in Figure 4.

(a) (b) (c) (d) (e) (f)

FIGURE 4. Image morphing between different images (a) source image (b) target image (c) morphed image ($\alpha = 0.1$) (d) morphed image ($\alpha = 0.5$) (e) morphed image ($\alpha = 0.8$) (f) restored target image

The source and the target images in Figure 4 are totally different. When the morphing rate is small, the quality of the morphed image is high, as shown in Figure 4(c). But when the morphed image is in the middle range, ghost shadows appear, as shown in Figure 4(d). Note that since the source and target images are totally different in the above experiment, there is no corresponding relationship between their features. Thus, the control points in the source image are selected arbitrarily. But to decrease the relocation noise, two control points with similar locations in the source and target images are selected as a pair of corresponding points. In addition, the reconstructed target image, as shown in Figure 4(f), is always identical to the original target image irrespective of the morphing rate.

4. **Proposed SIS Schemes Based on LIM.** In this section, two secret image sharing schemes based on the image morphing technique are proposed. The first scheme, a SIS scheme, shares a secret image with two shareholders. The second scheme extends the idea to share the secret image among n shareholders ($n > 2$).

4.1. **(2, 2) Secret image sharing.** A (2,2) secret image sharing scheme shares a secret image with two shareholders, and the secret image can be reconstructed under the condition that the two shareholders cooperate. For the proposed (2,2) SIS scheme, the secret image, I^{se}, acts as the target image in the morphing process. First, the dealer selects a share image, I_1^{sh}, which acts as the source image in the morphing process. Both I^{se} and I_1^{sh} have the same size. After that, r control points are selected from I_1^{sh}, and r corresponding control points are selected from I^{se}. The coordinates of the two groups of control points are recorded as C_1^{sh} and C^{se}, respectively. In addition, the dealer chooses a morphing rate, α. Finally, the dealer creates a morphed image using (10), i.e., $I_2^{sh} = \mathrm{LM}(I_1^{sh}, I^{se}, C_1^{sh}, C^{se}, \alpha)$. The morphed image, I_2^{sh}, acts as the second share in our (2,2) SIS scheme. The dealer sends the shares, I_1^{sh} and I_2^{sh}, to the shareholders secretly, and publishes α, C_1^{sh} and C^{se}, in which C_1^{sh} is associated with I_1^{sh}, and C^{se} is associated with I^{se}. The flowchart of the share generation is shown in Figure 5.

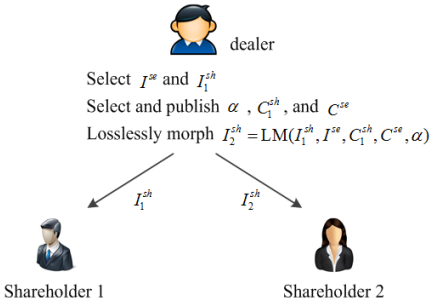


FIGURE 5. Share generation of the proposed (2,2) SIS scheme

As an alternative to publishing the morphing parameters, the dealer can send $[C_1^{sh}, \alpha]$ to shareholder 1 and send $[C^{se}, \alpha]$ to shareholder 2, together with the share images. When reconstructing the secret image, both shareholders must release their shares, I_1^{sh} and I_2^{sh}, and collect the morphing parameters, C_1^{sh}, C^{se}, and α. Then, the lossless demorphing algorithm shown as (13) is implemented by the shareholders, i.e., $I^r{-}^{se} = \mathrm{LD}(I_2^{sh}, I_1^{sh}, C_1^{sh}, C^{se}, \alpha)$. By this approach, the secret image is reconstructed. Figure 6 shows the experimental results of the proposed (2,2) SIS scheme, in which three groups of experiments were conducted. The first column in Figure 6 shows the first share, I_1^{sh}, which is also the source image in the morphing operation; the second column shows the second share, I_2^{sh}, which is the morphed image; the third column contains the secret image, I^{se}, which is the target image in the morphing operation; and the last column shows the reconstructed secret image, $I^r{-}^{se}$, which is identical to the original secret image.

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

FIGURE 6. Experimental results of the (2,2) SIS scheme (a) I_1^{sh} (b) I_2^{sh} (c) I^{se} (d) $I^r{-}^{se}$

The experimental results showed that the two shares were similar with the exception that there was a small amount of relocation noise in the second share. This is because that the morphing rate was in the source range. For the same reason, the morphed image looked natural irrespective of whether the source image and the target image was similar or not.

4.2. (n, n) **Secret image sharing.** In this section, an (n, n) SIS scheme based on image morphing is proposed, where $n > 2$. Assume that the secret image is I^{se} and that there are n shareholders. To share the secret image among the shareholders, the dealer chooses $n-1$ natural images, I_1^{sh}, I_2^{sh}, $\cdots$, I_{n-1}^{sh}, as shares. Both the secret image and the share images have the same size. Then, the dealer permutes the share images randomly as $I_{l_1}^{sh}$, $I_{l_2}^{sh}$, $\cdots$, $I_{l_{n-1}}^{sh}$, where $l_1, l_2, \cdots, l_{n-1}$ is a random permutation of $1, 2, \cdots, n-1$. The dealer selects r control points in each of the share images and the secret image and denotes their coordinates as $C_{l_1}^{sh}$, $C_{l_2}^{sh}$, $\cdots$, $C_{l_{n-1}}^{sh}$, and C^{se}. In addition, the dealer selects the morphing rates for each of the share images and denoted them as $\alpha_{l_1}^{sh}$, $\alpha_{l_2}^{sh}$, $\cdots$, $\alpha_{l_{n-1}}^{sh}$. Following that step, the dealer implements a sequential morphing operation, as shown in the follows:

$$\begin{aligned} I_1^m &= \mathrm{LM}(I_{l_1}^{sh}, I_{l_2}^{sh}, C_{l_1}^{sh}, C_{l_2}^{sh}, \alpha_{l_1}^{sh}), \\ I_2^m &= \mathrm{LM}(I_1^m, I_{l_3}^{sh}, C_{l_2}^{sh}, C_{l_3}^{sh}, \alpha_{l_2}^{sh}), \cdots, \\ I_{n-2}^m &= \mathrm{LM}(I_{n-3}^m, I_{l_{n-1}}^{sh}, C_{l_{n-2}}^{sh}, C_{l_{n-1}}^{sh}, \alpha_{l_{n-2}}^{sh}), \\ I_{l_n}^{sh} &= \mathrm{LM}(I_{n-2}^m, I^{se}, C_{l_{n-1}}^{sh}, C^{se}, \alpha_{l_{n-1}}^{sh}). \end{aligned} \tag{14}$$

In the sequential morphing algorithm shown as (14), first, the dealer generates an intermediate morphed image, I_1^m, using $I_{l_1}^{sh}$ as the source image and $I_{l_2}^{sh}$ as the target image. The second intermediate morphed image, I_2^m, is created using I_1^m as the source image and $I_{l_3}^{sh}$ as the target image. This process is implemented until the final morphed image, $I_{l_n}^{sh}$, is created using I_{n-2}^m as the source image and I^{se} as the target image. The share generation procedure can be depicted by Figure 7.

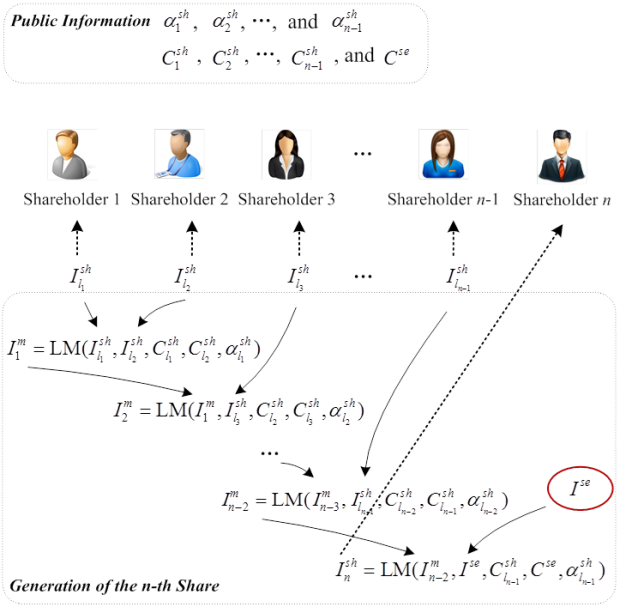


FIGURE 7. Share generation of the proposed (n, n) SIS scheme

To create the final morphed image, $I_{l_n}^{sh}$, the morphing operation is conducted sequentially $n-1$ times. The first $n-2$ morphing operations are conducted using the share images chosen by the dealer, and the last morphing operation involves the secret image. To share the secret image securely and to obtain a natural morphed image, $I_{l_n}^{sh}$, the following requirements must be satisfied:

- If the share images, $I_{l_1}^{sh}$, $I_{l_2}^{sh}$, $\cdots$, $I_{l_{n-1}}^{sh}$, have similar compositions, e.g., they are all human faces with similar sizes and positions, the morphing rates, $\alpha_{l_1}^{sh}$, $\alpha_{l_2}^{sh}$, $\cdots$, $\alpha_{l_{n-2}}^{sh}$,

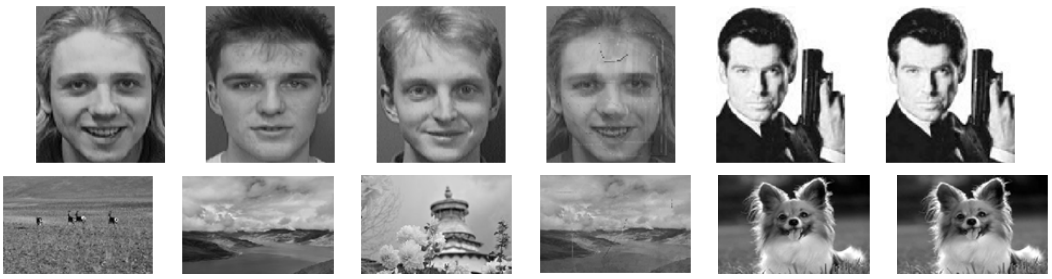
can be any values in the range of [0,1]. Meanwhile, the control points, $C_{l_1}^{sh}$, $C_{l_2}^{sh}$, $\cdots$, $C_{l_{n-1}}^{sh}$, should be corresponding, i.e., a group of control points, $c_{l_1}^{sh}(i)$, $c_{l_2}^{sh}(i)$, $\cdots$, $c_{l_{n-1}}^{sh}(i)$, should be located on the same feature position in each image ($c_{l_1}^{sh}(i) \in C_{l_1}^{sh}$, $c_{l_2}^{sh}(i) \in C_{l_2}^{sh}$,$\cdots$, $c_{l_{n-1}}^{sh}(i) \in C_{l_{n-1}}^{sh}$, and $i \in [1, r]$).

- If the share images, $I_{l_1}^{sh}$, $I_{l_2}^{sh}$, $\cdots$, $I_{l_{n-1}}^{sh}$, do not have similar compositions, the morphing rates, $\alpha_{l_1}^{sh}$, $\alpha_{l_2}^{sh}$, $\cdots$, $\alpha_{l_{n-2}}^{sh}$, must either be in the source range or be in the target range to decrease ghost shadows. In this situation, there is no need for the control points, $C_{l_1}^{sh}$, $C_{l_2}^{sh}$, $\cdots$, $C_{l_{n-1}}^{sh}$, to be corresponding.
- The secret image, I^{se}, can either be similar to or dissimilar from $I_{l_1}^{sh}$, $I_{l_2}^{sh}$, $\cdots$, and $I_{l_{n-1}}^{sh}$. To hide the secret image deeply, the last morphing rate, $\alpha_{l_{n-1}}^{sh}$, must be in the source range.

After the morphed image, $I_{l_n}^{sh}$, is created, the dealer updates the permutation of $l_1, l_2, \cdots, l_{n-1}$ by inserting n in a random location, e.g., $l_1, n, l_2, \cdots, l_{n-1}$. The new sequence, denoted as $l_1', l_2', \cdots, l_n'$, is a permutation of $1, 2, \cdots, n$. Since there are $n!$ different permutations of the sequence $1, 2, \cdots, n$, we number them from 1 to $n!$. The rule of numbering the permutations can be arbitrary but must be uniform among all of the shareholders and the dealer. Assuming that the number of the permutation $l_1', l_2', \cdots, l_n'$ is $\lambda(\lambda = 1, 2, \cdots, n!)$, the dealer generates $n-1$ random numbers, $\lambda_1, \lambda_2, \cdots, \lambda_{n-1} \in [1, n!]$, and computes $\lambda_n = \lambda - \lambda_1 - \lambda_2 - \cdots - \lambda_{n-1} \bmod n!$. Finally, the dealer transmits $< I_{l_i}^{sh}, \lambda_i >$ to the i^{th} shareholder $(i = 1, 2, \cdots, n)$.

When the n shareholders cooperate to reconstruct the secret image, first, they release the λ values. By computing $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n \bmod n!$, the permutation number λ can be obtained, and the morphing order for the first $n-2$ sequential morphing operation, $l_1, l_2, \cdots, l_{n-1}$, can be achieved. Then, the first $n-2$ morphing operations in (14) are conducted sequentially, and the intermediate morphing image, I_{n-2}^{m}, is obtained, which is the same as that in the share generation phase. Using I_{n-2}^{m} as the source image and I_n^{sh} as the morphed image, the LID operation, shown as (13), is implemented, and the secret image can be reconstructed, i.e., $I^r{-}^{se} = \mathrm{LD}(I_n^{sh}, I_{n-2}^{m}, C_{l_{n-1}}^{sh}, C^{se}, \alpha_{l_{n-1}}^{sh})$.

Some experiments of the proposed (n, n) SIS scheme were conducted in which $n = 4$, and two groups of experimental results are shown in Figure 8. In the figure, the first three columns contain the natural share images, I_1^{sh}, I_2^{sh}, and I_3^{sh}, which were selected by the dealer. The fourth column contains the final morphed image, I_4^{sh}, which was sequentially morphed by I_1^{sh}, I_2^{sh}, I_3^{sh}, and the secret image. The fifth column shows the secret image, I^{se}, and the last column shows the reconstructed secret image, $I^r{-}^{se}$. For the results of the first experiment that are shown in the first row in Figure 8, the morphing rates were $\alpha_1^{sh} = 0.4$, $\alpha_2^{sh} = 0.07$, and $\alpha_3^{sh} = 0.08$. Since I_1^{sh}, I_2^{sh}, and I_3^{sh} have similar structures, a natural morphed image, I_4^{sh}, can be created by choosing corresponding control points. For the results of the second experiment that are shown in the second row in Figure 8, since I_1^{sh}, I_2^{sh}, and I_3^{sh} do not have similar image structures, α_1^{sh} and α_2^{sh} must either be in the source range or the target range to diminish ghost shadows. Thus, we chose $\alpha_1^{sh} = 0.92$, $\alpha_2^{sh} = 0.09$, and $\alpha_3^{sh} = 0.05$. Note that in any case, α_3^{sh} must be in the source range to hide the secret image, I^{se}, deeply. The secret image can be reconstructed by implementing the LID operation to the morphed image, I_4^{sh}. The experimental results showed that the reconstructed secret image is identical to the original secret image.



(a) (b) (c) (d) (e) (f)

FIGURE 8. Experimental results of the (n, n) SIS scheme (a) share I_1^{sh} (b) share I_2^{sh} (c) share I_3^{sh} (d) share I_4^{sh} (e) secret image I^{se} (f) reconstructed secret image $I^r - ^{se}$

5. **Performance Comparison and Security.** In this section, we first compare the performances between the existing CBSIS schemes and the proposed scheme in Subsection 5.1. Then, we analyze the security of the proposed SIS scheme in two aspects. In Subsection 5.2, we demonstrate that the morphed image does not reveal the secret image. In Subsection 5.3, we prove that for the proposed SIS scheme, less than n shareholders cannot reconstruct the secret image.

5.1. **Performance comparisons.** This subsection compares the proposed scheme with four state-of-the-art SIS schemes, which are the scalable secret image sharing (SSIS) scheme [12], the essential secret image sharing (ESIS) scheme [13], the distortion-free secret image sharing (SFSIS) scheme [14], and the natural-image-based secret image sharing (NIBSIS) scheme [17].

The comparison results are shown in Table 1. Among these schemes, the SSIS, ESIS, and SFSIS schemes are all based on Shamir's polynomial function [11]. Although the polynomial-based schemes can losslessly reconstruct the secret image and usually decrease the share size, they generate noise-like shares, which tend to arouse attackers' attention. The SFSIS scheme solved this problem by embedding the noise-like shares into cover images as a watermark. However, the data that needed to be embedded was large, thus, this approach has the risk of being detected by steganalysis techniques.

The NIBSIS scheme has the similar idea with the proposed scheme, since both of them use $n-1$ natural images and the secret image to generate the n^{th} share. The difference between the two schemes is that, for the n^{th} share, the NIBSIS scheme uses a feature extraction algorithm to generate a noise-like image, while the proposed scheme uses image morphing algorithm to generate a natural image. Thus, the NIBSIS scheme actually provides partial meaningful shares. Although the authors of [17] proposed that the noise-like share can be hidden in a cover image as a watermark or be coded to Quick-Response (QR) code, both solutions lead to large suspicious information.

In addition, the (t, n)-threshold characteristic in Table 1 considers the relationship between t and n of the (t, n)-threshold secret sharing scheme. To reconstruct the secret image without any loss, only the ESIS scheme allows t to be less than or be equal to n, while the other methods are all (n, n) schemes, i.e., $t = n$ for lossless construction.

For the issue of share size, the schemes [14, 17], and the proposed scheme, which provide meaningful shares, all extend the size of share(s) to a certain extent. To achieve acceptable image quality, the parameter ρ in [14] should be small, which leads to large share size. The reason of size extension in [17] is converting the noise-like image to QR code, which also leads to large share size. Our proposed scheme is the first SIS scheme

that generates a natural share image. The output of (5) includes decimal numbers, thus, to losslessly reconstruct the secret image, more bits are used to represent a pixel of the morphed image. The size extension of the proposed scheme is moderate, compared with the existing schemes.

5.2. **Source range and target range.** In Section 3, we proposed the definitions of source range and target range. The security of our proposed SIS scheme lies in the fact that a morphed image that belongs to the source range does not reveal the secret image, i.e., the target image cannot be recognized from the morphed image.

To measure the dissimilarity between the original image, I^o, and the morphed image, I^m, we use the parameters of mean square error (MSE), peak signal-to-noise ratio (PSNR) in dB, and structural similarity (SSIM), which are defined as:

$$MSE(I^o, I^m) = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} [I^o(i,j) - I^m(i,j)]^2, \tag{15}$$

$$PSNR(I^o, I^m) = 10log_{10} \left(\frac{255^2}{MSE} \right), \tag{16}$$

$$SSIM(I^o, I^m) = \frac{(2\mu_o\mu_m + c_1)(2\sigma_{om} + c_2)}{(\mu_o^2 + \mu_m^2 + c_1)(\sigma_o^2 + \sigma_m^2 + c_2)}, \tag{17}$$

where μ_o and μ_m are the averages of the gray values of images I^o and I^m, σ_o^2 and σ_m^2 are the variances of I^o and I^m, σ_{om} is the covariance of I^o and I^m, c_1 and c_2 are two variables to stabilize the division with weak denominator. More details about the computation of SSIM can be found in [27]. In sum, two dissimilar images lead to high MSE value, low PSNR value, and low SSIM value.

Table 1. Performance comparison with the existing schemes

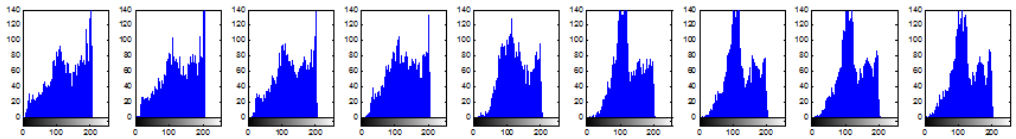
Properties	SSIS [12]	ESIS [13]	SFSIS [14]	NIBSIS [17]	The proposed scheme
Share generation Algorithm	Polynomial-based	Polynomial-based	Polynomial-based	Feature extraction	Image morphing
Meaningful shares	No	No	Yes when using watermarks	Partial	Yes
Lossless reconstruction	Yes	Yes	Yes	Yes	Yes
Average PSNR of shares	\	\	43 dB($\rho = 7$)	Not provided	35 dB for one share and INF for the others
Share size (times of secret image)	$\frac{2n-t}{n^2}$	$1/A$ for essential shares and B/A for the others	$\lceil log_\rho 255 \rceil$ (ρ is a prime number)	C for one share and 1 for the others	D for one share and 1 for the others
(t,n)threshold characteristic	$t = n$	$t \leq n$	$t = n$	$t = n$	$t = n$

A, B, C, and D are integers larger than one, and B is larger than A.

A large number of image morphing experiments using the proposed LIM algorithm were conducted, and two of them are shown in Tables 2 and 3. In the experiment as shown in Table 2, we chose similar original images, i.e., both the source image and the target image were human faces. In Table 3, we chose dissimilar source and target images to create the morphed images. The morphed images with various morph rates, i.e., 0, 0.05, 0.1, 0.2, 0.5, 0.8, 0.9, 0.95, and 1, were created. Note that when $\alpha = 0$, the morphed image is exactly the same as the source image; when $\alpha = 1$, the morphed image is the same as the target

image. The MSE, PSNR, and SSIM values between the source image and the morphed image, and the values between the target image and the morphed image, were calculated. The experiments show that when $\alpha < 0.1$, the histograms of the morphed image and the target image are different, and the values of $PSNR(I_T^o, I^m)$ and $SSIM(I_T^o, I^m)$ are low, which indicate that it is nearly impossible to distinguish the target image from the morphed image. In addition, the PSNR and SSIM between the source image and the morphed image are relatively high, which means the morphed image has relatively high quality. On the contrary, when $\alpha > 0.9$, it is nearly impossible to recognize the source image from the morphed image. Thus, we chose the source range as $\alpha_s = 0.1$ and the target range as $\alpha_t = 0.9$. The values of α_s and α_t may vary with the source and target images. Basically, the more dissimilar the source and target images are, the smaller α_s should be and the larger α_t should be. Since the target image serves as the secret image in our proposed SIS scheme, the secret image will not be revealed by a morphed image that belongs to the source range.

TABLE 2. MSE values between the morphed image and the original image (similar original images)

Morphing Rate	$\alpha = 0$	$\alpha = 0.05$	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$	$\alpha = 0.8$	$\alpha = 0.9$	$\alpha = 0.95$	$\alpha = 1$
I^m									
histogram									
$MSE(I_S^o, I^m)$	0	5.7	26.3	166.9	728.5	1380.3	1628.5	1778.8	2401
$MSE(I_T^o, I^m)$	2401	1764.5	1598.3	1295.5	662.0	138.5	33.3	5.2	0
$PSNR(I_S^o, I^m)$	INF	39.3	33.3	26.1	18.9	15.3	14.3	13.9	13.5
$PSNR(I_T^o, I^m)$	13.5	13.9	14.3	15.3	19.1	27.0	33.4	39.4	INF
$SSIM(I_S^o, I^m)$	1	0.9959	0.9849	0.9229	0.6994	0.5127	0.4576	0.4308	0.4035
$SSIM(I_T^o, I^m)$	0.4035	0.4269	0.4515	0.4994	0.6787	0.9236	0.9824	0.9954	1

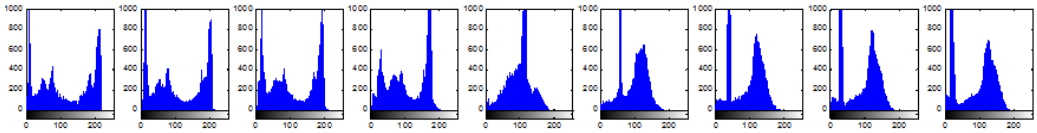
5.3. **Attacking tests.** In this section, we analyze the security of the proposed (n, n) SIS scheme under attack, and three attacking scenarios are analyzed and simulated as follows.

1) *Insufficient shareholders*

For the proposed (2,2) SIS scheme, it is apparent that neither I_1^{sh} nor I_2^{sh} can reconstruct the secret image separately. For the proposed (n, n) SIS scheme $(n > 2)$, if $I_i^{sh}(i = 1, 2, \cdots, n-1)$ is absent from the secret reconstruction, the intermediate morphed image in (14), I_{n-2}^m, will be different with that generated in the share generation phase. This means that for the last step of sequential morphing, the source image will be different from the image that was used in the share generation phase. Thus, the reconstructed image obtained by attackers, $I^r - ^{se}$, will be different from the original secret image, I^{se}.

To test the security of the proposed scheme under this kind of attack, we designed a (4,4) SIS scheme, for which the shares are shown as Figures 8(a), (b), (c), and (d) in the first row, and the secret image is Figure 8(e) in the first row. If one shareholder is absent from the secret reconstruction, e.g., the first shareholder, the

TABLE 3. MSE values between the morphed image and the original image (dissimilar original images)

Morphing Rate	$\alpha = 0$	$\alpha = 0.05$	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$	$\alpha = 0.8$	$\alpha = 0.9$	$\alpha = 0.95$	$\alpha = 1$
I^m									
histogram									
$MSE(I_S^o, I^m)$	0	33.0	1.3e+02	5.4e+02	3.4e+03	8.5e+03	1.1e+04	1.2e+04	1.0e+04
$MSE(I_T^o, I^m)$	1.0e+04	1.2e+04	1.1e+04	8.5e+03	3.4e+03	5.8e+02	1.3e+02	33.1	0
$PSNR(I_S^o, I^m)$	INF	31.8	25.5	19.6	11.7	7.7	6.7	6.2	5.7
$PSNR(I_T^o, I^m)$	5.7	6.8	7.2	8.2	12.2	19.9	26.2	32.3	INF
$SSIM(I_S^o, I^m)$	1	0.9817	0.9413	0.8383	0.5548	0.2810	0.1903	0.1458	0.1024
$SSIM(I_T^o, I^m)$	0.1024	0.1247	0.1496	0.2077	0.4500	0.8124	0.9340	0.9782	1

secret reconstruction will fail, as shown in the first row in Table 4. In this table, the reconstructed image obtained by attackers, $I^r - {}^{se\prime}$, is shown in the second column. In addition, the MSE, PSNR, and SSIM values between $I^r - {}^{se\prime}$ and the secret image, I^{se}, are computed. Experimental results show that the image reconstructed by attackers is chaotic, which does not reveal the information of the secret image.

2) *Incorrect sequential morphing order*

In this situation, all of the shadow images used by the attackers are correct, but the morphing order, $l'_1, l'_2, \cdots, l'_n$, is incorrect. An incorrect morphing order leads to different intermediate morphed images, thus the attackers cannot reconstruct the secret image. To simulate this attacking scenario, the shadow images shown as Figures 8(a), (b), (c) and (d) are used for a $(4, 4)$ SIS scheme, in which the order of the shadow image is 1, 2, 3, and 4. Let us assume that when the attackers reconstructed the secret image, they first used I_3^{sh} and I_2^{sh} to create the intermediate morphed image, I_1^m. Then, using I_1^m as the source image and I_1^{sh} as the target image, they created the intermediate morphed image I_2^m. Finally, using I_2^m as the source image and I_4^{sh} as the morphed image, the attackers reconstructed the secret image. Thus, the morphing order used by the attackers was 3, 2, 1, and 4. The reconstructed image obtained by the attackers is shown in the second row of Table 4. The experimental results show that using an incorrect morphing order leads to a chaotic reconstructed image.

3) *Incorrect share*

It is apparent that for a (n, n) SIS scheme, a different $I_i^{sh} (i = 1, 2, \cdots, n-1)$ leads to a different intermediate morphed image, $I_{n-2}^{m}{}'$, thus, the secret image cannot be reconstructed successfully. The reconstructed image under this attacking scenario is shown in the third row of Table 4, where the image shown as Figure 3(b) took the place of Figure 8 (a) to reconstruct the secret image. It is obvious that the reconstruction implemented by the attackers failed.

Table 4. Attacking tests

Attacking Scenario	$I^r - se'$	MSE	PSNR(dB)	SSIM
Insufficient shareholders		1.6e+04	6.11	0.0023
Incorrect sequential morphing order		1.5e+04	6.43	0.0141
Incorrect share		1.5e+04	6.29	0.0334

6. **Conclusions.** A novel (n, n) secret image sharing scheme using the image morphing technique was proposed in this paper, which shares a secret image with natural images. Using the proposed lossless image morphing algorithm, the secret image can be reconstructed accurately. Since the proposed lossless image morphing algorithm is sensitive to both the source image and the target image, the secret image cannot be constructed unless all of the shareholders cooperate.

Acknowledgment. Some of the facial images used in this paper were provided by the 'The ORL Database of Faces,' AT&T Laboratories, Cambridge.

REFERENCES

[1] M. Naor, and A. Shamir, Visual cryptography, in *Proc. Adv. Cryptology EUROCRYPT'94*, vol. 950, pp. 1-12, 1995.
[2] C. N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481-494, 2004.
[3] S. J. Shyu, and M. C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes, *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 960-969, 2011.
[4] D. S. Wang, L. Dong, and X. B. Li, Towards shift tolerant visual secret sharing schemes, *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 323-337, 2011.
[5] T. H. Chen, and K. H. Tsao, User-friendly random-grid-based visual secret sharing, *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1693-1703, 2011.
[6] X. T. Wu, and W. Sun, Random grid-based visual secret sharing with abilities of OR and XOR decryptions, *J. Vis. Commun. Image R.*, vol. 24, no. 1, pp. 48-62, 2013.
[7] X. T. Wu, and W. Sun, Generalized random grid and its applications in visual cryptography, *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1541-1553, 2013.
[8] Iwamoto, A weak security notion for visual secret sharing schemes, *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 372-382, 2012.
[9] K. H. Lee, and P. L. Chiu, An extended visual cryptography algorithm for general access structures, *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219-229, 2012.
[10] I. Kang, G. R. Arce, and H. K. Lee, Color extended visual cryptography using error diffusion, *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132-145, 2011.
[11] A. Shamir, How to share a secret, *Commun. ACM*, vol. 22, no. 11, pp. 612-613, 1979.
[12] Y. Y. Lin, and R. Z. Wang, Scalable secret image sharing with smaller shadow images, *IEEE Signal Process. Lett.*, vol. 17, no. 3, pp. 316-319, 2010.
[13] P. Li, C. N. Yang, C. C. Wu, Q. Kong, and Y. P. Ma, Essential secret image sharing scheme with different importance of shadows, *J. Vis. Commun. Image R.*, vol. 24, no. 7, pp. 1106-1114, 2013.

[14] P. Y. Lin, J. S. Lee, and C. C. Chang, Distortion-free secret image sharing mechanism using modulus operator, *Pattern Recognit.*, vol. 42, no. 5, pp. 886-895, 2009.
[15] C. C. Chang, Y. H. Chen, and H. C. Wang, Meaningful secret sharing technique with authentication and remedy abilities, *Inform. Sciences.*, vol. 181, no. 14, pp. 3073-3084, 2011.
[16] Aarti, H. K. Verma, and P. K. Rajput, Ideal contrast secret sharing scheme through meaningful shares with enveloping digital watermarking using bit plane based (k, n)-VCS, *Int. J. Comput. Appl.*, vol. 46, no. 9, pp. 36-41, 2012.
[17] K. H. Lee, and P. L. Chiu, Digital image sharing by diverse image media, *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 1, pp. 88-98, 2014.
[18] G. Wolberg, Skeleton-based image warping, *Visual Comput.*, vol. 5, no. 1-2, pp.95-108, 1989.
[19] T. Beier, and S. Neely, Feature-based image metamorphosis, in *Proc. SIGGRAPH*, pp.35-42, 1992.
[20] L. Zhu, Y. Yang, S. Haker, and A. Tannenbaum, An image morphing technique based on optimal mass preserve mapping, *IEEE Trans. Image Process.*, vol. 16, no. 6, pp.1481-1495, 2007.
[21] S. S. Lin, I. C. Yeh, C. H. Lin, and T. Y. Lee, Patch-based image warping for content-aware retargeting, *IEEE Trans. Multimedia*, vol. 15, no. 2, pp.359-368, 2013.
[22] S. Faisan, N. Passat, V. Noblet, R. Chabrier, and C. Meyer, Topology preserving warping of 3-D binary images according to continuous one-to-one mappings, *IEEE Trans. Image Process.*, vol. 20, no. 8, pp.2135-2145, 2011.
[23] N. Stefanoski, O. Wang, M. Lang, P. Greisen, S. Heinzle, and A. Smolic, Automatic view synthesis by image-domain-warping, *IEEE Trans. Image Process.*, vol. 22, no. 9, pp.3329-3341, 2013.
[24] H. K. Tso, T. M. Lo, and W. K. Chen, Friendly medical image sharing scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 3, pp. 367-378, 2014.
[25] C. C. Chen, and Y. H. Tsai, An expandable essential secret image sharing structure, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 1, pp. 135-144, 2016.
[26] Q. Mao, K. Bharanitharan, and C. C. Chang, Edge directed automatic control point selection algorithm for image morphing, *IETE Technical Review*, vol. 30, no. 4, pp. 336-343, 2013.
[27] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600-612, 2004.