Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2010, Article ID 593236, 18 pages
doi:10.1155/2010/593236

Research Article

Meaningful Share Generation for Increased Number of Secrets in Visual Secret-Sharing Scheme

Mustafa Ulutas

Department of Computer Engineering, Karadeniz Technical University, 61080 Trabzon, Turkey

Correspondence should be addressed to Mustafa Ulutas, ulutas@ieee.org

Received 3 October 2009; Revised 20 March 2010; Accepted 17 May 2010

Academic Editor: Panos Liatsis

This paper presents a new scheme for hiding two halftone secret images into two meaningful shares created from halftone cover images. Meaningful shares are more desirable than noise-like (meaningless) shares in Visual Secret Sharing because they look natural and do not attract eavesdroppers' attention. Previous works in the field focus on either increasing number of secrets or creating meaningful shares for one secret image. The method outlined in this paper both increases the number of secrets and creates meaningful shares at the same time. While the contrast ratio of shares is equal to that of Extended Visual Cryptography, two secrets are encoded into two shares as opposed to one secret in the Extended Visual Cryptography. Any two natural-looking images can be used as cover unlike the Halftone Visual Cryptography method where one cover should be the negative of the other cover image and can only encode one secret. Effectiveness of the proposed method is verified by an experiment.

1. Introduction

Internet is one of the most popular but insecure communication mediums. People use the internet for all kinds of communication needs including VOIP, peer-to-peer file sharing, up-to-date news reading, e-commerce, and online transactions. Since it is an open and insecure medium, malicious users can intercept data when people transmit personal information. The fast growth of online applications results in the data security problem, which is an important issue for all users. In order to achieve data security, users need secure communication methods for transmitting secret messages over the Internet. Steganography is one of the methods for hiding secret data in a cover medium such as a digital image, a video, or an audio file. Since the cover medium is a meaningful file, attackers do not know that it has hidden data [1–5]. Therefore, malicious users will not pay attention to the file to retrieve the secret data. Encryption is another well-known method for achieving data security. It transforms secret information into an encrypted form, which looks like a random message. Transformation procedure is called encryption process and the result is called cipher text.

Encryption makes the message unreadable, making message suspicious enough to attract eavesdroppers' attention [1]. A computational device is required to perform decryption of the cipher text. Therefore, the cost or efficiency of the hardware is mostly proportional to the security level of the encryption algorithm. Thus, stronger encryption algorithms need hardware with more processing power.

Visual Cryptography (VC) is another technique for achieving data security [6]. It is a cryptographic method in which cipher text can be decoded directly by the human visual system. Decryption process does not require any special calculation or computational device. Thus, it eliminates the drawback of hardware and software requirement, which is essential for the decryption process in traditional cryptography. In VC [6], one secret image is encoded into n shares that contain seemingly random pictures and are distributed to participants. Each participant cannot retrieve any information from his own transparency, but when at least k of them superimpose their transparencies pixel by pixel, they retrieve the secret from the superimposed result by using their visual system. Such a scheme is called "(k, n) visual secret sharing (VSS)" by Naor and Shamir [6]. Any k transparencies can be stacked to retrieve secret. Stacking of $k - 1$ or less does not reveal the secret. Retrieved secret's contrast, when k or more transparencies are superimposed, is proportional to the number of superimposed transparencies. Such an interesting scheme's decryption process requires only human visual system instead of any computational device. It is much useful in situations where computing devices are not available or not possible to use [7].

After this pioneering research, some of the works done focused on the contrast (the relative difference in hamming weight that comes from the stacking result of white pixel and black pixel) or construction of the VSS schemes for binary images [8–13]. These applications use the binary images as input due to the requirements of the proposed model. Some of the works focused on this problem and extended VSS schemes to support grayscale or color images [14–16]. Other studies show how to create shares to be meaningful pictures to make the method friendly and less noticeable [17–23]. Unfortunately, these applications use only one confidential message to embed. In order to solve the shortcoming, researchers have proposed methods, which increased the number of secrets [24–27].

Wu and Chen proposed a scheme to embed two secret images into two shares in visual cryptography [24]. Two sets of confidential messages can be embedded via rotating a specific share. Stacking result of two shares called by S_1 and S_2 reveals the first share, denoted by $S_1 \otimes S_2$. Second secret becomes visible if the first share is rotated counterclockwise by θ, denoted by S_1^{θ} and stacked together with S_2. Shares used by this study are rectangular, which makes only four angles possible for perfect alignment of pixels. There is a pitfall in their scheme reported by [26]: they decompose S_1 into four triangular regions of equal areas. Since the encoded pixels in each of the four areas are the same, S_1 is not a random picture. In fact, only $1/4$ of the extended blocks in S_1 are purely random.

Wu and Chang improved this study by designing the shares to be circular [25]. Therefore, restrictions of the rotation angles can be relaxed. Rotation angle can be any value within $(0°, 360°)$. However, strictly speaking, first share produced by this research is also not totally random picture. Some of the works done in recent years focused on hiding more than two secrets. In [26], Shyu et al. proposed a method that can decode multiple secrets in two circular shares different from those of the previous works [24, 25]. Another work, a visual secret-sharing scheme that uses two shares for hiding multiple secrets, is also proposed [27].

However, all these methods produce noise-like shares. In other words, shares have no visual meaning, hinder the objectives of visual cryptography, and invite illicit attempts [18, 20]. Some methods are proposed in recent years to overcome this problem [17–23].

In [23], hypergraph colorings are used to construct meaningful shares as binary images for one secret image. This work, called "Extended Visual Cryptography," deals with binary images. In [17], Nakajima and Yamaguchi proposed a method that establishes this technique for natural images. Nevertheless, their proposed scheme takes three pictures as input and generates two of them as shares. Third picture, namely, the secret, is obtained by stacking two meaningful shares together. In [19], Yue and Chiang proposed a neural network approach to generate meaningful shares. This scheme provides gray level shares and gray level decoded secret. In [20], Zhou et al. propose a halftone visual cryptography scheme and provide shares with visual information. Visual quality of the shares produced by this method has been improved in [21, 22]. The method in [20] requires two shares but one of them must be the negative of the other. A view of the earth from space, meaningful in both positive and negative, is used for testing, but natural images are not appropriate for this method. Shares created by well-known standard test images such as Lena or Baboon would look negative and invite illicit attempts.

However, all these schemes that produce meaningful shares can be used to embed only one secret. Some schemes code multiple secrets into two shares [24–27]. However shares still look like noise images in these methods. Other studies that generate meaningful shares in the literature can code only one secret [17–23]. Therefore, there is a tradeoff between the number of secrets and meaning of shares. In the literature, research is focused on either to increase the number of secrets or to create meaningful shares with one secret. Our method satisfies these two constraints at the same time.

We increase the number of secrets produced by Extended Visual Cryptography [23]. Different from the previous works, two secrets can be embedded into meaningful shares. We also utilize the Wu and Chen coding algorithm to produce fully random share images [28]. Randomness problem in this method is reported by Shyu et al. [26]. Rectangular shares are used in the proposed scheme. First share is produced in a fully random manner as opposed to Wu and Chen's algorithm. Since proposed method produces the first share in a fully random manner, second share can use extended blocks represented by six different patterns. However, Wu and Chen's second share contains only four different patterns because of the first share being composed of exactly the same four regions. The method makes use of two cover images to create friendly shares. Cover and secret images are of the same size. Meaningful shares do not draw attention like random shares. Thus, eavesdroppers do not suspect that meaningful shares contain any secret.

The rest of this paper is organized as follows. In Section 2, we review the visual secret-sharing schemes proposed by Wu and Chen. The proposed scheme is introduced in Section 3. The experimental results and discussions are presented in Section 4. Finally, the conclusions and some concluding remarks are given in Section 5.

2. Chen and Wu's VSS Scheme

Chen and Wu proposed a new (2, 2) visual secret-sharing scheme in 1998. It encrypts two secrets into two shares using share rotation technique. Angle of rotation can only be 90°, 180°, or 270° since shares are square and overlap pixel by pixel for only these rotations. Two $N \times N$ halftone secret images are expanded by a factor of 2 in each dimension. In other words, each pixel in secrets is expanded to 2×2 extended block to create two shares of size $2N \times 2N$ that will reveal no information about secret images. First secret becomes visible if first and second shares are stacked together. Second secret becomes visible if first share is rotated CCW by 90° and stacked with second share. Wu and Chen assume that the first share can be segmented

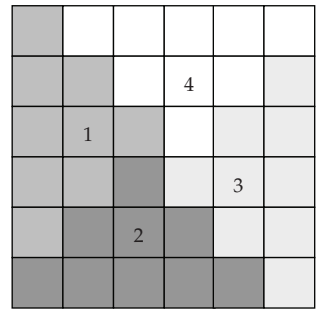


Figure 1: Triangular regions in the first share of 6 × 6 pixels.

Figure 2: Four patterns to be assigned.

into four regions of triangular shape with equal contents. Triangular regions for a first share of size 6×6 pixels are illustrated in Figure 1. Each 2×2 extended block of the first region in the first share is randomly selected from one of the 2 × 2 patterns in Figure 2. Extended blocks in other regions are assigned to be the same as corresponding extended block in the first region.

At the beginning, they create first share to constitute four triangular regions with equal contents. Each region contains $(N \times N)/4$-extended blocks. Extended blocks of all four triangular regions are exactly the same to simplify the scheme. Let block j in region k be denoted as b_j^k for $1 \le k \le 4$ and $1 \le j \le (N \times N)/4$. Extended blocks in the first region are selected in a fully random manner and are copied to corresponding extended blocks in other regions. That is, $b_j^t = b_j^1$ for $t = 2, 3, 4$ and $1 \le j \le (N \times N)/4$. Extended blocks of the second share must be defined according to the value of the corresponding extended blocks of the first share and the pixel values at the relative positions in secret images.

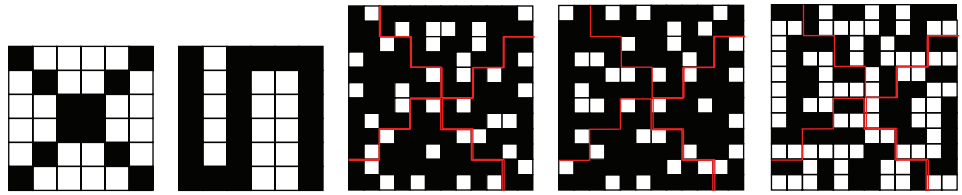
We explain how Wu and Chen's encoding process works by using a simple example. Two secret images and two shares created after encoding process are denoted by P_1, P_2, S_1, and S_2, respectively. Rotation result of the first share by θ is denoted by $S_1^{\theta^\circ}$. Rotation angle will be assumed to be 90° in this example. For simplicity, two secret images of size 6 × 6 pixel are used to create 12 × 12 pixel shares after encoding process. First share can be decomposed into four triangle-like areas where each area has nine extended blocks as shown in Figure 3. Extended blocks labeled with the same number have the same contents to illustrate the dependency.

Let us pay attention to the first pixels at the top left in P_1 and P_2. Assume that those pixels in P_1 and P_2 are (■, ■) as shown in Figure 4. Assume that corresponding block b_1^1 at first share is randomly determined as ◧, then as mentioned b_1^2, b_1^3, b_1^4 are assigned to be the same as b_1^1. Corresponding extended block of b_1^1 at $S_1^{90^\circ}$ is the rotation result of ◧, namely ◪. Corresponding extended block in S_2 must reveal black when stacked with extended blocks at S_1 and $S_1^{90^\circ}$, respectively.

Therefore, the pattern that satisfies this constraint is selected among four different patterns (⬒, ⬓, ◧, ◨) that have two white and two black pixels. If the corresponding extended block at S_2 is selected as ⬒, stacking this pattern with (◧, ◪), respectively, will reveal the extended blocks that have four black subpixels, which seem black to human visual system.

1	5	4	3	2	
2	6	8	7	6	5
3	7	9	9	8	4
4	8	9	9	7	3
5	6	7	8	6	2
1	2	3	4	5	1

Figure 3: First share of size 6 × 6 pixel and four triangular regions that have nine extended blocks.



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

Figure 4: (a) P_1, (b) P_2, (c) S_1, (d) $S_1^{90^\circ}$, and (e) S_2.

As can be seen in the above example, extended blocks at the first area will be selected randomly, and the other three areas' contents will be the same. Therefore, each extended block of the $S_1^{90^\circ}$ is the rotated result of the corresponding extended block at S_1.

Therefore, Wu and Chen know the corresponding extended block of an extended block at the first share, when the share is rotated. Contrary to proposed method, the table illustrating possible extended blocks for combinations of secret image pixels is definite in their scheme. Let Figure 6(a) represent the first share where each extended block is denoted as a_i for $1 \leq i \leq 36$, and Figure 6(b) represents the rotation result of first share. (a_1, a_6), (a_6, a_{36}), (a_{31}, a_1), and (a_{36}, a_{31}) are corresponding extended blocks as can be seen in Figure 6.

Therefore, selected pattern that paints extended block denoted by a_1 affects the selection of the pattern that paints the extended block a_{31} during creation of the first share. Actually, there exist dependencies in the selection of the patterns that paint these four extended blocks. An example will show this problem clearly. If a_1 and a_6 are selected in a fully random manner to be (◪, ◩) and first pixels of the two secret images are (□, ■), respectively, then rotation result of a_6, that is ◪, will be the corresponding extended block of a_1. Therefore, corresponding extended blocks at S_1 and $S_1^{\theta^\circ}$ are (◪, ◪). In that case, there is no pattern appropriate (to reveal □, ■) for corresponding extended block at S_2. None of the S_2 patterns, when stacked with these extended blocks, reveal pixel values (□, ■) of two secret images since hamming distance among these two extended blocks is 0. Hamming distance must be either one or two because hamming weight of the patterns to construct the second share is two. Hamming distance cannot be one because all the patterns that will be used for painting the first share have three black pixels and one white pixel. Difference in one pixel due to rotation will result in a hamming distance of two.

Chen and Wu's algorithm selects the same pattern to paint these four extended blocks (a_1, a_6, a_{31}, and a_{36}) as shown in the example above. When their scheme is applied, same

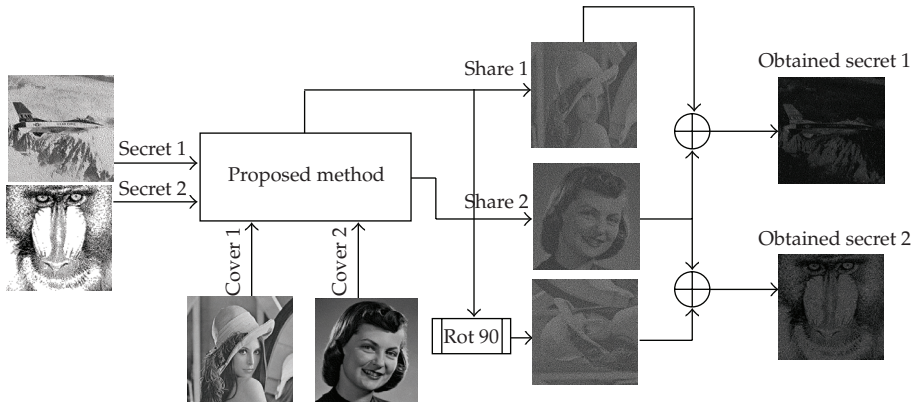


Figure 5: Coding and decoding phases of the proposed algorithm.

pattern will be used to paint both a_1 and a_6. If a_1 and a_6 are selected to be (◪, ◪), respectively, corresponding extended blocks at S_1 and $S_1^{\theta^\circ}$ will be (◪, ◪). Any S_2 pattern can be selected for corresponding extended block at S_2, since hamming distance between these two extended blocks is two. Hamming distance among the corresponding extended blocks will always be two since extended blocks will overlap with their rotated result. All combinations of pixel values (represent the corresponding pixel value of two secret images) can be coded by selecting an appropriate S_2 pattern.

As can be seen in the above example, Wu and Chen segment the first share into four triangular-shaped regions of equal areas. Since rotated pattern of an extended block in S_1 and corresponding extended block in $S_1^{90^\circ}$ must be the same, an extended block pattern is copied to all extended blocks in S_1 that overlap by rotation. That is, $(b_j^k) = (b_j^{4-k+1})$ for $k = 1$ and $(b_j^k) = (b_j^{k-1})^{90^\circ}$ for $k = 2, 3, 4$. Their second share consists of only four out of six possible patterns excluding diagonals.

As a result, Wu and Chen's algorithm does not need to take into account the dependencies among the extended blocks by copying the same pattern for extended blocks that overlap by rotation. There is an important pitfall in their scheme due to limited randomness of the first share. Since corresponding pixels in each triangular-shaped area are assigned to the same value, first share is not fully random. Only a quarter of the first share is random and the rest of the share is an exact copy of the first triangular area. However, an important issue in the implementation of secret-sharing schemes is the amount of randomness required for generating the shares [26]. Proposed method in this paper creates the first share in a fully random manner as will be explained in the third section of this paper.

3. Proposed Method

In visual secret-sharing schemes for multiple secrets, each share is a form of random distributed black and white pixels (is indistinguishable from random noise). The inconvenience of these schemes is that they use meaningless shares to hide the secrets. A novel (2, 2) visual secret-sharing scheme with meaningful shares is proposed in this section.

Proposed method takes two secret and two cover images as shown in Figure 5. Cover images are used for construction of the meaningful shares. Two secret images are

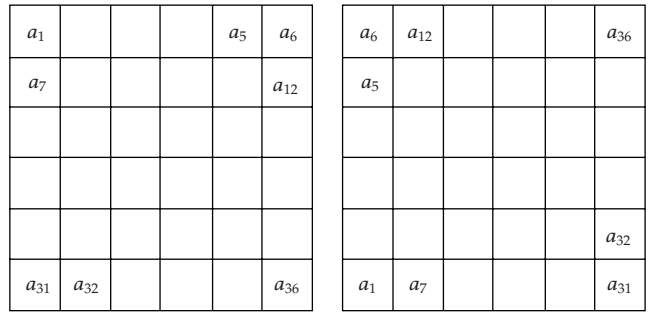


Figure 6: (a) S_1 and (b) $S_1^{90^\circ}$.

reconstructed by using these two meaningful shares. First share is constructed by using the two secret images and two cover images while second share is constituted by using the two secret images and second cover image.

During the decoding process, the first secret image becomes visible by just stacking the two shares. The second secret is revealed, after rotating the first share by θ degrees and stacking it with the second share. Proposed algorithm constructs the first share in a fully random manner different from Wu and Chen's algorithm. Therefore, pixel values (black or white) of the cover images can be used for construction of the corresponding extended blocks in meaningful shares. If pixel value in cover image is black at a certain position, the 2×2 extended block of a share at that position should have one white and three black pixels. It means that the extended block appears like black as in cover image. If the pixel value is white in cover image, extended block at that position in a share has two white and two black pixels that appear white. Pattern selection process in an extended block will be explained in detail below. When two shares are stacked together, if all of the four subpixels in the 2×2 extended block are black, this block represents a black pixel in the secret image. If one white pixel exists in the extended block, this extended block would represent a white pixel.

Hiding two secret images into two covers by the proposed scheme is more efficient than concatenation of two secret images into a single and larger image and then sharing it. Let secret images be of size $N \times N$. Concatenation of these images will result in an $N \times 2N$ image. The size of resulting shares would be $2N \times 4N$ if Shamir's visual secret-sharing approach is used. However, the proposed method generates shares of size $2N \times 2N$ with the same hiding capacity. Thus, the proposed method is preferable in terms of storage capacity and bandwidth requirements.

3.1. Generation of the First Share

It is supposed that A and B denote the first and second shares, respectively. Besides, let S_1, S_2, C_1, C_2 denote the first and second secrets and cover images of k bit depth, respectively. These four images of size $N \times N$ are transformed into halftone images of only black and white pixels.

We first define two different pattern groups, namely, P_b, P_w, to be used during share generation process. Pattern groups are the basic constituents of the shares. There are one white and three black pixels in each pattern of the P_b, and two white and two black pixels

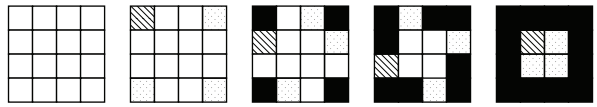


Figure 7: (a), (b), (c), (d), and (e) represent the strolling process for a 4×4 secret image and $\theta = 90°$.

in P_w. Six different combinations for P_w and four different combinations for P_b exist. Each extended block of shares is filled according to these patterns by checking the corresponding pixels of both cover images. For instance, if the cover-image pixel value is black, then the extended block type in a share can be selected from P_b. Otherwise, block type is determined among the patterns in P_w. This will guarantee generation of meaningful shares at the cost of reduced contrast of cover images.

One should be careful about the order of extended blocks to be set in the first share since the pattern of an extended block will also affect another extended block at the corresponding position when the share is rotated. A Boolean matrix denoted by T of the same size as secrets is used in order to determine the pixel in a secret that has to be processed during the creation of the first share. All the elements of T are initialized to False (0) indicating unprocessed pixels at the beginning. We define a procedure that scans T through rows starting from the leftmost column. First False value's location gives the starting point of the *strolling process* that will be explained later. Scanning T as explained above yields $(1, 1)$ as the starting point to the strolling process at the beginning. n pixels are processed during each call of the strolling process and corresponding elements (n elements) of T are set to True (1).

The value of n depends on the angle of rotation of the first share. During the strolling process, starting point will be processed at first. After that, new coordinates obtained by the rotation transform of starting point's coordinates will be the new pixel position to be processed. New pixel is evaluated if the corresponding value (designated by the new coordinates) at T is False. Strolling process terminates when the transformation yields the same pixel evaluated in the beginning of the strolling process and corresponding value of T is True which means "processed previously." Because of the nature of the rotation transform, last point will be the starting point after n transforms. For example, let θ be 90°. In that case, last point will be the starting point after four transformations. So n is 4, 2, 4 for 90°, 180°, 270°, respectively. Example illustration of this strolling process for a secret image of size 4×4 pixels is given in Figure 7.

As can be seen in this example, rotation angle determines the number of steps, represented by n, during the strolling process. New coordinates at each step will give the position of the pixels to be taken into account at secret and cover images during strolling process. Extended block at the corresponding position in first share (A) is determined as follows.

An extended block in A must be defined according to a corresponding 2×2 extended block in the rotated A, namely, A', and the pixel values at the relative position of the secrets and cover images. When A and A' stack with second share (B), the first and second secret images are obtained, respectively. Thus each corresponding extended block pair in A and A' will be used while constructing secret images' pixel values at that position. Therefore, if we can select appropriate values for extended blocks in A and A', corresponding extended block in B is easily determined.

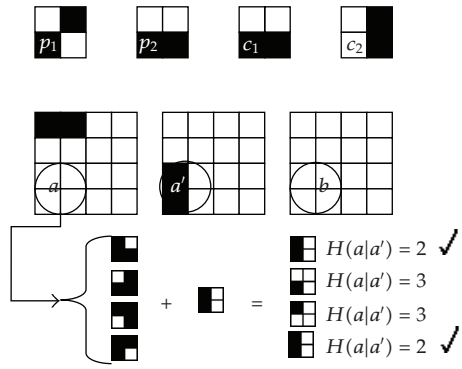


Figure 8: Determination of an extended block at the first share.

For the purpose of illustration, assume that two corresponding pixel values at two secret images for an extended block (namely, a) in A are the (■, ■) and called p_1 and p_2, respectively, as shown in Figure 8. These two pixels must be obtained during decoding process via stacking corresponding extended block at (A, B) and (A', B), respectively. Let corresponding pixel values at cover images (C_1, C_2) be (■, □) and let them be called c_1 and c_2. Pixel values at cover images are used in the selection of the pattern for the extended blocks (let a, a', b be the corresponding extended blocks in A, A', and B, resp.).

In this example, because c_1 is ■, P_b will be used for the selection of the pattern which will be placed into a. It is to say that extended block, namely, a, contains three black and one white pixel. Besides, let a' be the ◧. In order to determine the most appropriate pattern for a, the value of c_2 must be taken into account since c_2 will affect the selection of the pattern that will be used for painting the corresponding extended block (b) in B. One pattern that seems appropriate for painting a can be an inappropriate candidate for b. Assume that a will be selected randomly as ◪.

As mentioned above, a' was ◧. An appropriate pattern for b will be selected from P_w since c_2 is white. The selected pattern for b stacked with a and a' should result in four black pixels that seem black to the human visual system because p_1 and p_2 are black. Whereas, hamming weight of OR'ed a and a' vectors results in 3 giving the number of the white pixels. Since c_2 is white (has only two black pixels), any pattern for c_2 could not be able to cover these three pixels. In other words, both of $a \otimes b$, $a' \otimes b$ do not reveal black. One can define a rule, that is, "hamming weight of the selected pattern for a OR'ed with a' should be less than or equal to the two," for the construction of an extended block in the first share. This rule is valid for only (p_1, p_2 = ■, ■) and (c_1, c_2 = ■, □). Determination of appropriate extended blocks that can paint b is shown in Figure 8.

As can be seen in this example, pattern selection for an extended block in first share effects the creation of second share. Therefore, the pattern that paints an extended block in the first share may not be selected in a fully random manner. *Selection process* takes into account two secret images and two cover images at the same time to determine the appropriate patterns. Thus, the pattern that will paint an extended block in a first share can be selected randomly among the set of patterns resulting from the selection process.

The rule set can be defined as follows by using the pixel values at secret images and cover images. Which pattern group (P_b or P_w) to be tested with this rule set is determined by the corresponding pixel value at first cover image. Hamming weight of the OR'ed vectors a

and a' is denoted by $H(\mathrm{OR}(a, a'))$, like the hamming weight of AND'ed vectors that denoted by $H(\mathrm{AND}(a, a'))$.

(i) *Rule* 1. "If p_1 is *black*, p_2 is *black*, $H(\mathrm{OR}(a, a'))$ is less or equal to 3, and c_2 is *black*," then it is an appropriate pattern.

(ii) *Rule* 2. "If p_1 is *black*, p_2 is *black*, $H(\mathrm{OR}(a, a'))$ is less or equal to 2, and c_2 is *white*," then it is an appropriate pattern.

(iii) *Rule* 3. "If p_1 is *white*, p_2 is *white*, $H(\mathrm{AND}(a, a'))$ is greater or equal to 1, and c_2 is *black*," then it is an appropriate pattern.

(iv) *Rule* 4. "If p_1 is *white*, p_2 is *white*, and c_2 is *white*," then it is an appropriate pattern.

(v) *Rule* 5. "If p_1 is *white*, p_2 is *black*, and $H(\mathrm{XOR}(a, a'))$ is greater than 1," then it is an appropriate pattern.

(vi) *Rule* 6. "If p_1 is *black*, p_2 is *white*, and $H(\mathrm{XOR}(a, a'))$ is greater than 1," then it is an appropriate pattern.

(vii) *Rule* 7. Otherwise, it is an inappropriate pattern.

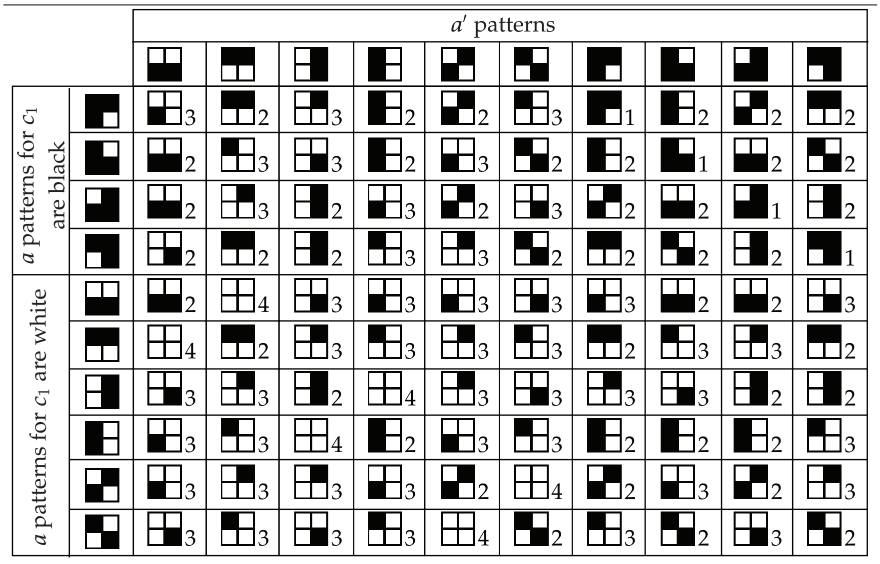
Extended blocks at coordinates obtained by strolling process will be determined by using this rule set. n-extended block in each step during strolling process will be determined. Therefore, strolling process will be called $(N \times N)/n$ time for an $N \times N$ secret image. Each execution of strolling process will constitute n-extended block of the first share.

The constraints on the construction of the first share may give an impression that the selection process may not be able to select an appropriate pattern (denoted by a in Figure 8) for extended blocks at coordinates obtained by the strolling process. The rules given in the selection process are also generated from the requirements of coding both p_1 and p_2 by taking care of the values of c_1 and c_2. For example, the reason to select a hamming weight of a or a' less or equal to 3 in Rule 1 depends on two criterions; corresponding pixels in both secret images are black and corresponding cover pixel in the second cover image is black. Therefore, selectable patterns for corresponding extended block in the second share b should have exactly three black pixels and one white pixel to both cover a and a' at the same time and to yield black p_1 and black p_2 pixels when overlapped.

It is easy to prove that an appropriate pattern can always be selected by inspecting outcomes of the visual results of the 6 rules given in the selection process. There are a total of 10 different patterns, 6 to represent white and 4 to represent black pixels. In other words, a and a' can contain one of the $C_1^{10}C_1^{10} = 100$ possible pattern combinations. Hamming weights of OR'ed, AND'ed, and XOR'ed a and a' patterns are given in Tables 1, 3, and 5, respectively. Six rules use these weights to decide whether a pattern is appropriate for a taking into account c_2. Tables 2, 4, and 6 list all appropriate patterns that can be used for determining a. There exists at least one solution for any p_1, p_2, c_1, and c_2 as can be seen in Tables 2, 4, and 6. Since hamming weight criterion in all rules takes generation of appropriate b into account, at least one solution for b is guaranteed.

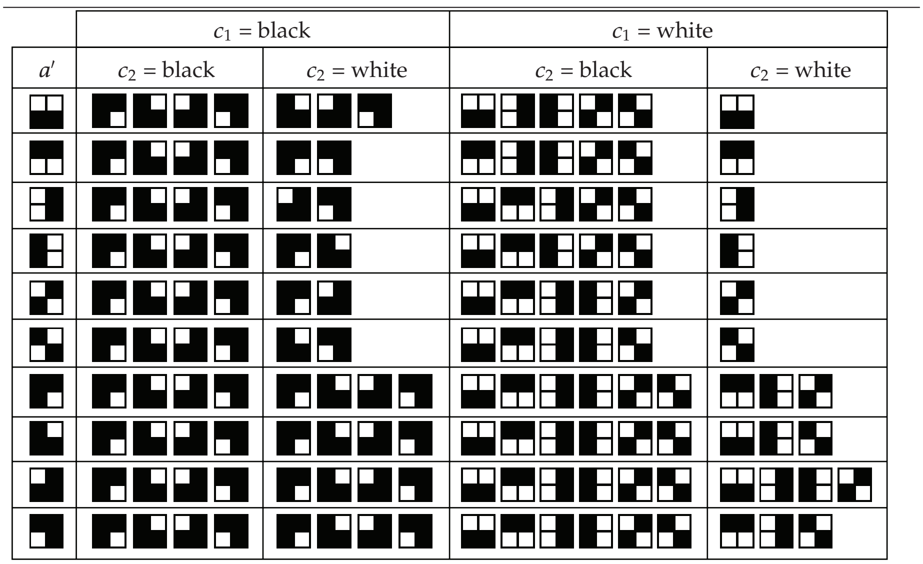
The security capability of the proposed method can be analyzed by inspecting these tables. In general VSS schemes, owners cannot extract any information about the secret by inspecting patterns in their shares. Likewise, patterns used for coding the white secret pixels are also used for coding the black secret pixels with equal probability as in general VSS. In the proposed scheme, 10 different patterns are used in both shares to code four different possible combinations of the two secret pixels in regards of cover image pixels. Tables 2, 4, and 6 show the possible solutions for black p_1 and black p_2, for white p_1 and white p_2, and for mutually

Table 1: Result of $H(OR(a, a'))$ for all possible conditions in Rules 1, 2.



a patterns	a' 1	a' 2	a' 3	a' 4	a' 5	a' 6	a' 7	a' 8	a' 9	a' 10
a patterns for c_1 are black (1)	3	2	3	2	2	3	1	2	2	2
a patterns for c_1 are black (2)	2	3	3	2	3	2	2	1	2	2
a patterns for c_1 are black (3)	2	3	2	3	2	3	2	2	1	2
a patterns for c_1 are black (4)	2	2	2	3	3	2	2	2	2	1
a patterns for c_1 are white (1)	2	4	3	3	3	3	3	2	2	3
a patterns for c_1 are white (2)	4	2	3	3	3	3	2	3	3	2
a patterns for c_1 are white (3)	3	3	2	4	3	3	3	3	2	2
a patterns for c_1 are white (4)	3	3	4	2	3	3	2	2	2	3
a patterns for c_1 are white (5)	3	3	3	3	2	4	2	3	2	3
a patterns for c_1 are white (6)	3	3	3	3	4	2	3	2	3	2

Table 2: Selectable a patterns for Rules 1, 2 according to both c_1 and c_2.



exclusive p_1 and p_2 secret pixels, respectively. Since 10 possible patterns exist in all these tables, one cannot conclude the secret pixels' values by just inspecting his/her own patterns. In other words, patterns existing in shares do not reveal any information about the two secret images encoded by them.

3.2. Generation of the Second Share

Contrary to share A generation, share B generation does not require a strolling process. Extended blocks of first share A are scanned through columns. One extended block from A

Table 3: Result of $H(AND(a, a'))$ for all possible conditions in Rules 3, 4.

		a' pattern									
a pattern for c_1 is black		0	1	0	1	1	0	1	0	0	0
		1	0	0	1	0	1	0	1	0	0
		1	0	1	0	1	0	0	0	1	0
		0	1	1	0	0	1	0	0	0	1
a pattern for c_1 is white		2	0	1	1	1	1	0	1	1	1
		0	2	1	1	1	1	1	0	0	1
		1	1	2	0	1	1	0	0	1	1
		1	1	0	2	1	1	1	1	0	0
		1	1	1	1	2	0	1	0	1	0
		1	1	1	1	0	2	0	1	0	1

Table 4: Selectable a patterns for Rules 3, 4 according to both c_1 and c_2.

	c_1 = black		c_1 = white	
a'	c_2 = black	c_2 = white	c_2 = black	c_2 = white

and corresponding extended block at A' are taken into account together at each step during scanning process. Let a and a' be the patterns that paint the relative extended blocks at A and A', respectively. b is defined as a pattern that will paint corresponding extended block at second share. Relative pixel values at two secret images must be obtained when b is stacked with a and a', respectively. Therefore, b should be selected according to both a and a'.

Appropriate patterns for b can be selected among the patterns at P_b or P_w. Relative pixel value at the second cover image determines pattern group to be used in order to create shares that look like cover images. Therefore, shares are meaningful images and do not draw

Table 5: Result of $H(XOR(a, a'))$ for all possible conditions in Rules 5, 6.

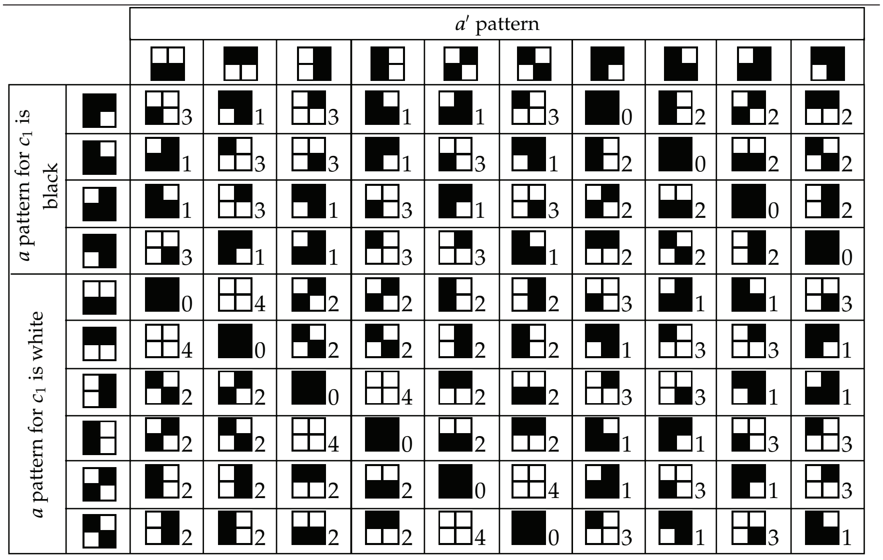
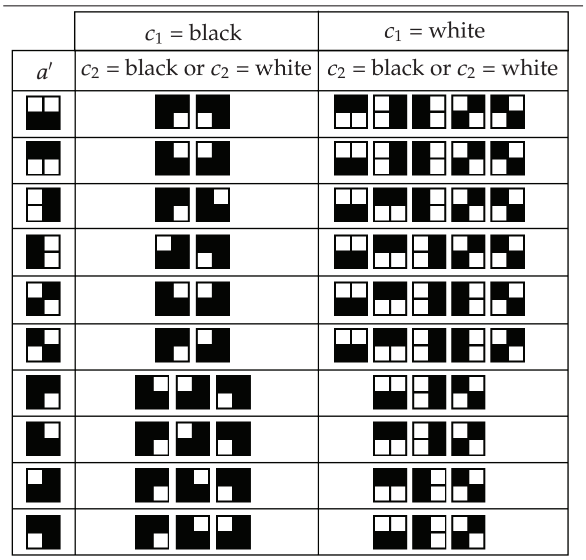


Table 6: Selectable a patterns for Rules 5, 6 according to both c_1 and c_2.



eavesdroppers' attention. Even though shares are meaningful, contrast of the cover images is reduced by a factor of 4.

Initially, all patterns that belong to a selected pattern group (P_b or P_w) are candidate for b. Only a set of appropriate patterns could reveal original pixel values of both secret images. A rule base is defined to find this appropriate pattern set as follows. Let p_1 and p_2 be pixel values of two secret images and let c_2 be the pixel value of second cover image, respectively.

(i) *Rule* 1. If p_1 is *black*, p_2 is *black*, $H(\mathrm{AND}(a,b))$ is 0, and $H(\mathrm{AND}(a',b))$ is 0, then it is an appropriate pattern.

(ii) *Rule* 2. If p_1 is *black*, p_2 is *white*, $H(\mathrm{AND}(a,b))$ is 0, and $H(\mathrm{AND}(a',b))$ is not 0, then it is an appropriate pattern.

(iii) *Rule* 3. If p_1 is *white*, p_2 is *black*, $H(\mathrm{AND}(a,b))$ is not 0, and $H(\mathrm{AND}(a',b))$ is 0, then it is an appropriate pattern.

(iv) *Rule* 4. If p_1 is *white*, p_2 is *white*, $H(\mathrm{AND}(a,b))$ is not 0, and $H(\mathrm{AND}(a',b))$ is not 0, then it is an appropriate pattern.

Patterns selected according to these rules are appropriate for painting the corresponding extended block at B. A random selection can be made among this pattern set. Therefore selected pattern for corresponding extended block at B will reveal both p_1 and p_2 when stacked with a and a', respectively. Since both extended blocks at A' and pixel values of c_2 are taken into account while determining the extended blocks at A during creation of the first share, there is at least one solution for corresponding extended block at B. Second share created by the procedure outlined above looks similar to second cover image, because pattern groups to be tested are selected according to the relative pixel values of second cover image as explained before.

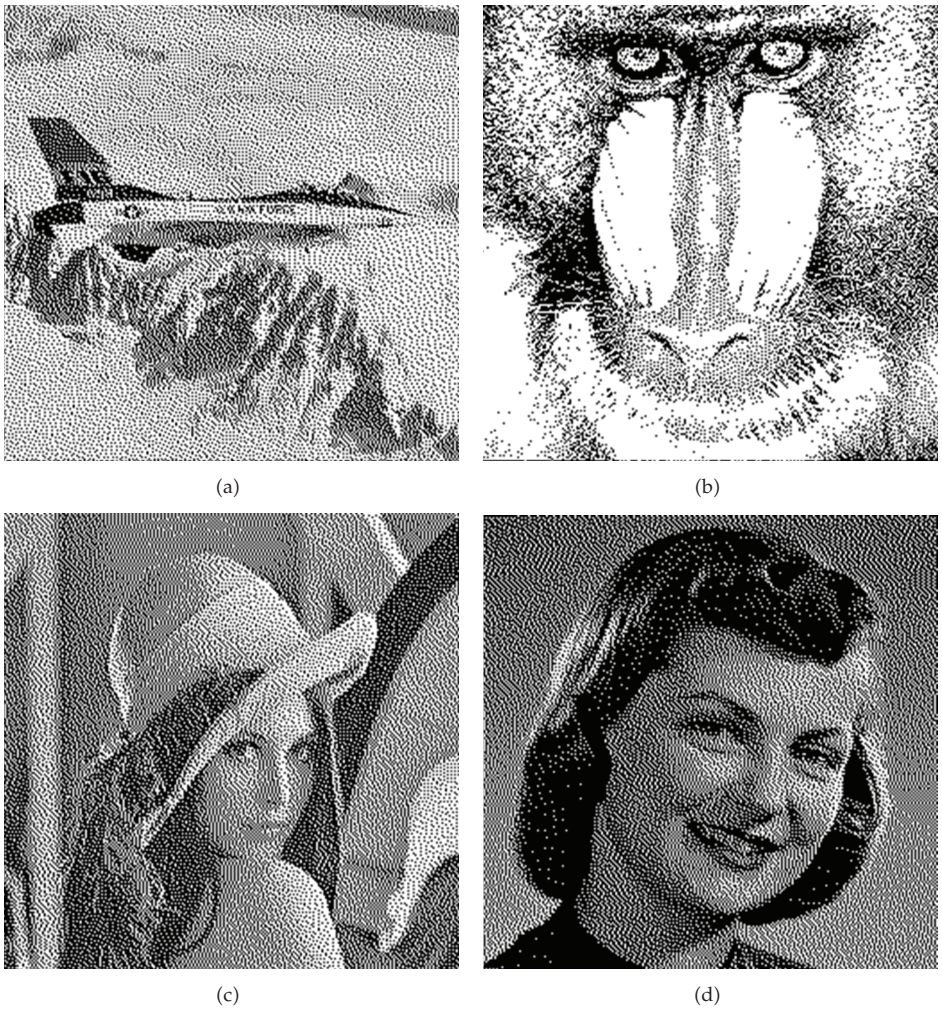
4. Experimental Results and Analysis

In order to check the validity of the proposed scheme, four gray level test images (two for secret images and two for cover images) given in Figure 11 are used to create meaningful shares and then reconstruct the secrets. Baboon and Jet, two well-known test images of size 256×256, are used as secret images given in Figures 9(a) and 9(b). Figures 9(c) and 9(d) show two cover images of size 256×256, "Lena" and "Girl," respectively.

Proposed method is coded in Matlab 7.0 running on Windows XP Professional computer. GIMP, an open-source image processing application, is used to create Floyd-Steinberg halftone secrets. Since each secret pixel is represented by a 2×2 extended block at meaningful shares, the expansion factor is 4. Meaningful shares created by the proposed scheme are given in Figure 10. Rotation angle of 90° is used but other rotation angles given in Section 3.1 could also be used for the method. First secret is revealed when first and second shares are stacked together whereas second secret is obtained if first share is rotated CCW by 90° and stacked with the second share as shown in Figures 11(a) and 11(b), respectively.

Shares' extended blocks corresponding to black pixels at cover images are represented by three black pixels and one white pixel whereas those corresponding to white pixels have only two black and two white pixels. Therefore, contrast of the cover images is reduced by four, since contrast is the difference between the revealed black and white pixels.

Proposed method's contrast ratio is equal to the contrast ratio of "Extended Visual Cryptography" method. In spite of this equality, our method can embed two secrets into two shares, while Extended Visual Cryptography can only encode one secret. Our method uses two different natural images as the cover image, whereas one meaningful share and its negative must be used in [20], and can only encode one secret. Shares created by this method attract attention of the eavesdropper if a natural image such as Lena is used. Our method can make use of any two different cover images to create shares. Creating natural-looking shares is an important feature of the method to escape illicit attempts. Hiding more than one secret and using two different natural cover images are the superiority of our method different from



(a) (b)

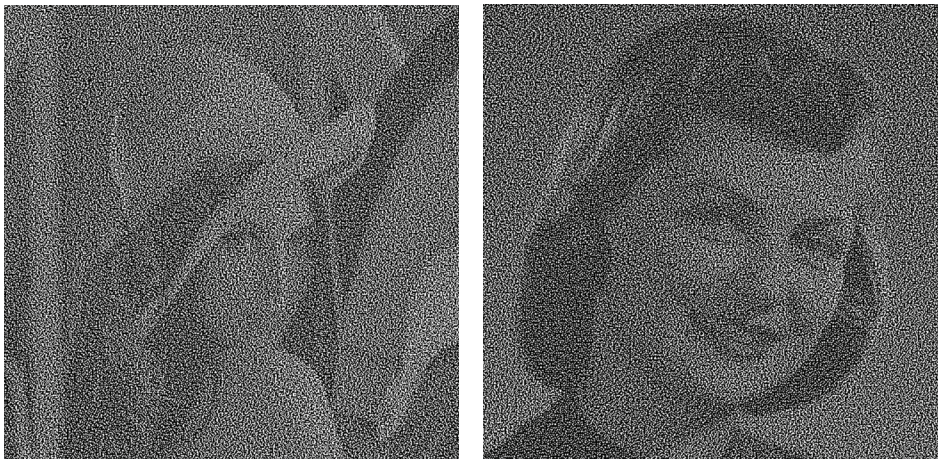
(c) (d)

Figure 9: (a) First secret, (b) second secret, (c) first cover image, and (d) second cover image.

the work in [20]. So, two parameters (meaningful shares and number of secret) are utilized by our approach. While our method encodes two secrets, it can also create meaningful shares from two different natural cover images.

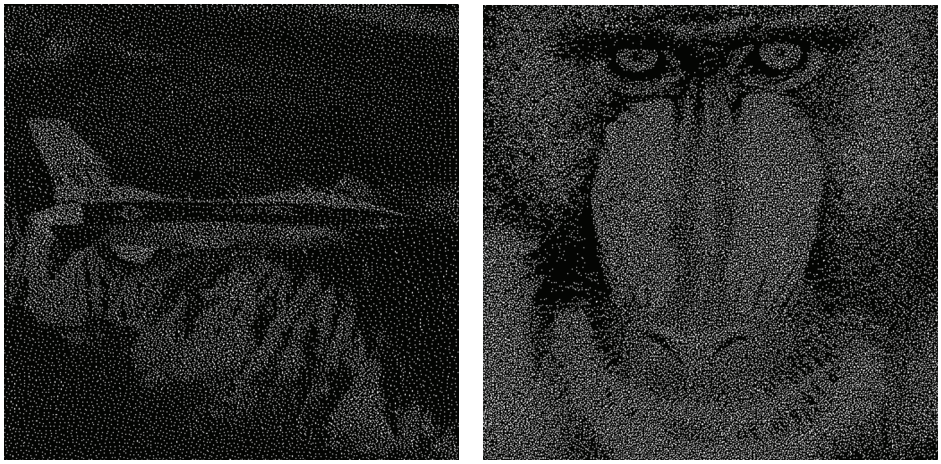
5. Conclusion

Traditional Visual Cryptography encodes the secret into meaningless, noise-like shares. Shares of this nature draw the attention of the malicious users and are not easy to manage [18]. Therefore, research is focused on creating meaningful shares in recent years. Extended Visual Cryptography proposed by Atenies et al. [23] was the milestone in creating meaningful shares. However, this method can encode only one secret into meaningful shares. Some research based on this work is about enhancing the visual quality of meaningful shares [20–22]. VSS schemes that generate meaningful shares dealt with embedding only one secret.



(a) (b)

Figure 10: Meaningful shares, S_1 and S_2, created by proposed method.



(a) (b)

Figure 11: Secrets revealed by stacking shares: (a) $S_1 \otimes S_2$ and (b) $S_1^{90^\circ} \otimes S_2$.

VSS schemes that can encode multiple secrets create meaningless shares. Our objective is both increasing the number of secrets and creating meaningful shares at the same time.

A novel (2, 2) Visual Secret-Sharing Scheme is proposed in this paper. Encoding two secrets in two meaningful shares is performed by using share rotation principle introduced by Wu and Chen in [24]. Even though their method creates two seemingly random shares, the first share is only 1/4 random as reported in [26]. In order to create truly random shares, a new encoding scheme, also used in [28], is utilized and proved to be successful. Creating truly random shares is important for the generation of meaningful shares. Should the first share not be created in a fully random manner, only 1/4 of the share look similar to cover, and other parts will be the rotated result of it contradicting with the friendliness of the share.

Experimental results prove that two cover images and two secrets can be used to create two meaningful shares that look like cover images with decreased contrast ratio. First

secret is revealed by stacking two shares, whereas rotating the first share CCW by 90° and stacking with the second share reveal the second secret. The average Peak Signal Noise Ratio (PSNR) of shares created with the proposed algorithm with respect to their original halftones (cover images) is 3.59 dB. This value is equal to PSNR obtained by the shares with Extended Visual Cryptography. With the same visual appearance of meaningful shares, our method can encode two secrets while EVC can encode one secret.

The proposed method works for two secrets to generate two shares with 2×2 pixel expansion as 90° rotation, and perfectly aligning square-shaped shares are assumed. Embedding more than two secrets into meaningful shares and improving the visual quality of both the shares and secrets are considered as a future work.

References

[1] C.-C. Chang and H.-W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognition Letters*, vol. 25, no. 12, pp. 1431–1437, 2004.

[2] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[3] S. Wang, B. Yang, and X. Niu, "A secure steganography method based on genetic algorithm," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 28–35, 2010.

[4] F.-X. Yu, H. Luo, and S.-C. Chu, "Lossless data hiding for halftone images," *Studies in Computational Intelligence*, vol. 227, pp. 181–203, 2009.

[5] F.-H. Wang, J.-S. Pan, and L. C. Jain, "Digital watermarking techniques," *Studies in Computational Intelligence*, vol. 232, pp. 11–26, 2009.

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

[7] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, vol. 40, no. 12, pp. 3633–3651, 2007.

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, pp. 86–106, 1996.

[9] D. R. Stinson, "An introduction to visual cryptography," in *Presented at Public Key Solutions '97*, Toronto, Canada, April 1997.

[10] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes and Cryptography*, vol. 11, no. 2, pp. 179–196, 1997.

[11] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *Journal of Cryptology*, vol. 12, no. 4, pp. 261–289, 1999.

[12] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," in *Proceedings of the 3rd Annual international Conference on Computing and Combinatorics*, vol. 1276, pp. 176–185, 1997.

[13] S. Cimato, R. De Prisco, and A. De Santis, "Colored visual cryptography without color darkening," *Theoretical Computer Science*, vol. 374, no. 1–3, pp. 261–276, 2007.

[14] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, no. 7, pp. 1619–1629, 2003.

[15] C.-C. Lin and W.-H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognition Letters*, vol. 24, no. 1–3, pp. 349–358, 2003.

[16] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, vol. 39, no. 5, pp. 866–880, 2006.

[17] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," in *Proceedings of the 10th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision (WSCG '02)*, pp. 303–340, University of West Bohemia, Plzen, Czech Republic, 2002.

[18] G. Horng, D. S. Tsai, and T. Chen, "On generating meaningful shares in visual secret sharing scheme," *Imaging Science Journal*, vol. 56, no. 1, pp. 49–55, 2008.

[19] T.-W. Yue and S. Chiang, "A known-energy neural network approach for visual cryptography," in *Proceedings of the International Joint Conference on Neural Networks (IJCNN '01)*, vol. 4, pp. 2542–2547, Washington, DC, USA, July 2001.

[20] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2441–2453, 2006.

[21] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via direct binary search," in *Proceedings of the 14th European Signal Processing Conference (EUSIPCO '06)*, Florence, Italy, September, 2006.

[22] Z. Wang and G. R. Arce, "Halftone visual cryptography via through error diffusion," in *Proceedings of the International Conference on Image Processing*, pp. 109–112, October 2006.

[23] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science*, vol. 250, no. 1-2, pp. 143–161, 2001.

[24] C. C. Wu and L. H. Chen, *A study on visual cryptography*, M.S. thesis, Institute of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, 1998.

[25] H.-C. Wu and C.-C. Chang, "Sharing visual multi-secrets using circle shares," *Computer Standards & Interfaces*, vol. 28, no. 1, pp. 123–135, 2005.

[26] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, vol. 40, no. 12, pp. 3633–3651, 2007.

[27] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognition*, vol. 41, no. 12, pp. 3572–3581, 2008.

[28] M. Ulutaş, R. Yazici, V. V. Nabiyev, and G. Ulutaş, "(2,2)-secret sharing scheme with improved share randomness," in *Proceedings of the 23rd International Symposium on Computer and Information Sciences (ISCIS '08)*, Istanbul, Turkey, October 2008.