International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 7, October 2014, PP 101-113
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Encrypting Digital Images and Using Diverse Image Media for Sharing Digital Images

Minal Nerkar

Department of Computer Engineering
Savitribai Phule Pune University
Ganeshkind, Pune
nerkar.minal@gmail.com

Kshitij Naik

Department of Computer Engineering
Savitribai Phule Pune University
Ganeshkind, Pune
aissmsioit@hotmail.com
k.naik70@gmail.com

Taniya Rohmetra

Department of Computer Engineering,
Savitribai Phule Pune University
Ganeshkind,
Pune
taniya_rohmetra@yahoo.co.in

Sayali Saste

Department of Computer Engineering
Savitribai Phule Pune University
Ganeshkind, Pune
sayali.saste@gmail.com

Tejan I*rla*

Department of Computer Engineering
Savitribai Phule Pune University
Ganeshkind, Pune
tejanirla4@gmail.com

Abstract: *Visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images, but it will arouse suspicion and increase risk during transmission. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. The natural shares can be photos or hand-painted pictures in digital form. To address this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. The noise-like share is generated based on these shares and the secret image. The unaltered natural shares greatly reduce the transmission risk problem. We also put forward a way to hide the noise like share called Steganography. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.*

Keywords: *Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk, steganography.*

1. INTRODUCTION

VISVAL cryptography (VC) is a technique that encrypts a secret image into *n* shares, with each participant holding one or more shares. Anybody who holds fewer than *n* shares cannot reveal any information about the final secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human eyes.

Secret images can be of various types: images, photographs, handwritten documents, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in non-computer-aided environments; however, devices with computational powers are ubiquitous (e.g., smart phones). Thus, sharing visual secret images in computer-aided environments has become an important issue today. Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents, but they will suffer from two drawbacks: first, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be

intercepted. Thus, the risk to both the participants and the shares increases, in turn increasing the probability of transmission failure. Second, the meaningless shares are not user friendly. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares. Previous research into the Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme provided some effective solutions to cope with the management issue. The shares contain many noise-like display low-quality images or pixels. Such shares are easy to detect by the naked eye, and participants who transmit the share can easily lead to suspicion by others. By adopting steganography techniques, secret images can be concealed in cover images that are halftone gray images and true-color images However, the stego-images still can be detected by steganography analysis methods. Therefore the existing VSS schemes still must be investigated for reducing the transmission risk problem for carriers and shares. A method for reducing the transmission risk is an important issue in VSS schemes.

In this study, we propose a VSS scheme, called the natural image–based VSS scheme (NVSS scheme), to reduce the intercepted risk during the transmission phase. Basically, conventional VSS schemes use a unity carrier (e.g., either transparencies or digital images) for sharing images, which limits the practicality of VSS schemes. In the proposed scheme, we explore the possibility of using diverse media for sharing digital images. The carrier media in the scheme contains printed images, digital images, hand-painted pictures, and images taken from a camera so on. Applying a diversity of media for sharing the secret image increases the degree of difficulty of intercepting the shares. The proposed NVSS scheme can share a digital secret image over n . 1 arbitrary natural images (hereafter called natural shares) and one share. So there is no need of altering the contents of the natural images, the proposed approach extracts or selects features from each natural share. These unaltered natural shares are totally innocuous, thus greatly reducing the interception probability of these shares. The generated share that is noise-like can be concealed by using data hiding techniques to increase the security level and makin it more secure as well as easy to send during the transmission phase.

The NVSS scheme uses diverse media as a carrier; hence it has many possible scenarios for sharing secret images. For example, we will assume a dealer selects n .1 media as natural shares for sharing a secret image. To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media i.e. the user can use any normal image (e.g., hand-painted pictures, pictures taken from a camera, landscape, portrait photographs, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras, computers, laptops, tablets or even a smart phones) to reduce the risk of being suspected. The printed media (e.g., hand-painted pictures or flysheets) can be sent via postal or direct mail marketing services or even my e-mail. In such a way, the transmission channels are also diverse, further reducing the transmission risk and thus increasing the security for the images.

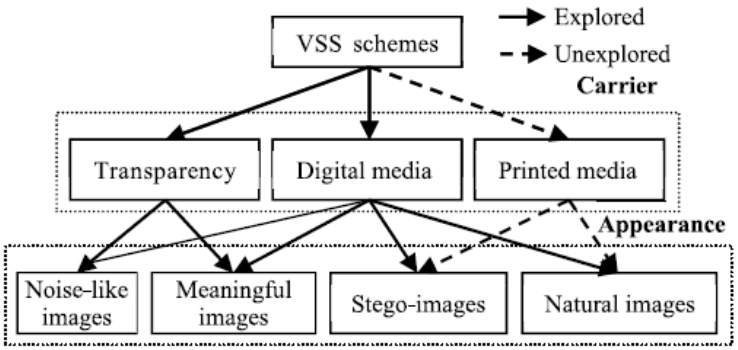


Fig1. *Classification of VSS schemes*

In this paper, we develop efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares.

The remainder of this paper is organized as follows.

Section II reviews the framework of the research done. In Section III, we present the proposed NVSS scheme. The encryption/decryption algorithms are proposed in Section IV. In Section V, the security and performance of the proposed NVSS scheme are evaluated by experiments. Finally, we present the conclusions of this work in Section VI.

2. RELATED WORK

Fig. 1 shows the classification of VSS schemes from the carriers' viewpoints. Existing research focuses only on using transparencies or digital media as carriers for a VSS scheme. The transparency shares have either a a meaningful appearance or noise-like appearance. The conventional noise-like shares are not friendly, hence, the researchers tried to enhance the friendliness of VSS schemes for participants . Generally, very simple easy to understand and meaningful cover images are added to noise-like shares for identification of the image, making traditional VC schemes more user friendly and manageable. However, the EVCSs reduce the display quality of the recovered images. Research has focused on gray-level and color secret images to develop a user-friendly VSS scheme that adds cover images into the meaningless shares. To share our secret and other digital images, VSS schemes use digital media as carriers, which makes the appearance of the shares more variable and more user-friendly. Many of the papers have investigated meaningful halftone shares and emphasized the quality of the shares more than the quality of the recovered images. These studies had serious side effects in terms of poor display quality for the recovered images and pixel expansion, although the display quality of the shares was enhanced. Hence, researchers make a tradeoff between the quality of the recovered images, the quality of the shares, and the pixel expansion of the images.

Research has further focused on color and gary-level secret images to develop a user-friendly VSS scheme that will add cover images into the meaningless shares. To share digital images, VSS schemes use digital media as carriers, which makes the appearance of the shares more variable and more user-friendly. Several papers investigated meaningful halftone shares and emphasized the quality of the shares more than the quality of the recovered images. These studies had serious side effects in terms of pixel expansion and poor display quality for the recovered images, although the display quality of the shares was enhanced. Hence, researchers make a tradeoff between the quality of the shares, the quality of the recovered images, and the pixel expansion of the images. In another research branch, researchers used steganography techniques to hide secret images in cover images. Basically, steganography is defined as the technique of hiding information and making the communication invisible. In this way, no one who is not involved in the transmission of the information suspects the existence of the information. Digital shares have been successfully hidden by using steganography. Therefore, the hidden information and its carrier can be protected. Steganography has been used to hide digital shares in VSS schemes. The shares in VSS schemes are embedded in cover images to create stego-images. Although the shares are totally concealed and the stego-images have a high level of user friendliness, the shared information and the stego-images remain intercepted risks during the transmission phase.

Recently, Kshitij Naik et al. tried to share a secret image via natural images. This was a very first attempt to share images via natural images; however, this work may suffer a problem—the textures of the natural images could be disclosed on the share. Moreover, images that have been already printed are difficult to use, printed images cannot be used for sharing images in the previous scheme. So far, sharing visual secret image via unaltered printed media remains to still be an open problem. In this study, we make an extension of the previous work to promote its practicability and explore the possibility for adopting the unaltered printed media as shares.

3. THE PROPOSED SCHEME

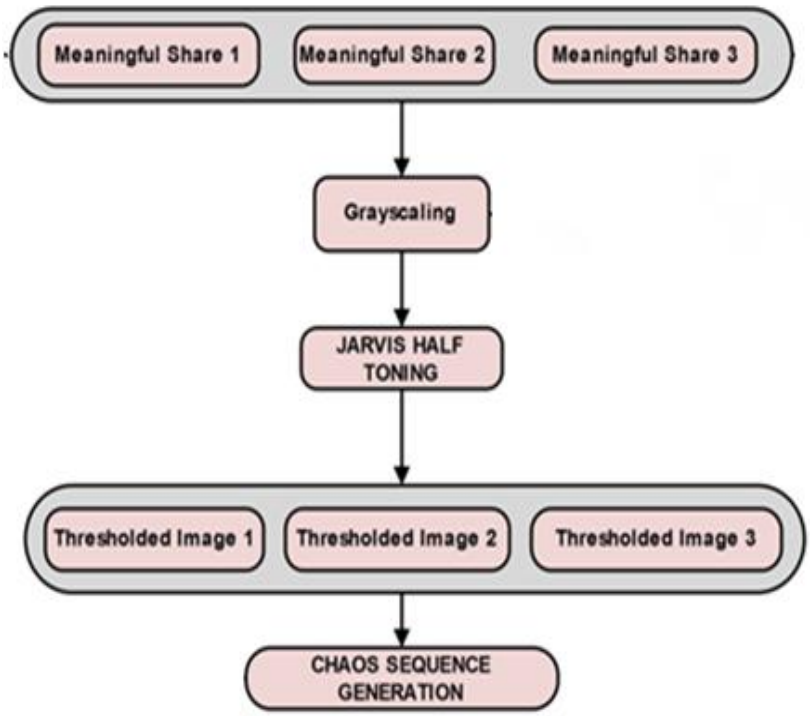
3.1. Background

In cryptography, the one-time pad (OTP), which was proven to be impossible to break only if it was used correctly, was developed in 1917 by Gilbert Vernam. Each character or bit from the plain text is encrypted by a modular addition (or a logical XOR operation) with a character or bit from a secret random key of the same length as the plain text resulting in a cipher text. Ciper text is something like a password that is indeed necessary. The cipher text was sent to a receiver; then, the original plaintext can be decrypted in the receiver side by applying the exactly same operation and the exact same secret key as the sender used for encrypting the cipher text. As pointed out by Naor and Shamir, the visual secret sharing scheme is similar to the OTP encryption system. In a 2, 2_-VSS scheme, the secret

random key and the cipher text that can be treated as two shares in the scheme were distributed to two participants who involve in the scheme. The two participants can decrypt the secret by applying the decryption operation to the shares that were held by the participants. In this study, we adopt the notion of the OTP technique to share the digital visual secrets. Instead of generating a secret random key, we extract the secret key from an arbitrarily picked natural image in the .2, 2_-NVSS scheme. The natural image and the generated share (i.e., cipher text) were distributed to two participants. In decryption process, the secret key will be extracted again from the natural image and then the secret key as well as the generated share can recover the original secret image. The .2, 2_-NVSS scheme can be extended to the .*n*, *n*_-NVSS scheme by adopting *n* . 1 natural images for generating *n* . 1 secret keys. Thus, in such a way, the visual secret image can be shared by the *n*. 1 natural images as well as the generated share.

3.2. The Proposed.n, n-NVSS Scheme

As Fig. 2(a) shows, the encryption process of the proposed (*n*, *n*)-NVSS scheme, *n* . 2, includes two main phases: feature extraction and encryption. In the feature extraction phase, 24 binary feature images are extracted from each natural share. The natural shares (N1,…, N*n*.1.include np printed images (denoted as ***P***) and nd digital images (denoted as ***D***), np . 0, nd . 0, np .nd .1 and *n* .np .nd .1. The feature images (F1,..., F*n*.1.that were extracted from the some natural image subsequently are combined to make one feature image with 24-bit/pixel color depth. In the encryption phase, the *n* . 1 feature images (F1,..., F*n*.1.with 24-bit/pixel color depth and the secret image execute the XOR operation to generate one noise-like share S with 24-bit/pixel color depth. Then, to reduce the transmission risk of share S, the share is concealed behind cover media or disguised with another appearance by the data hiding process. The resultant share S.is called the generated share. The *n* . 1 innocuous natural shares and the generated share are *n* shares in the (*n*, *n*)-NVSS scheme. When all *n* shares are received, the decryption end extracts *n* .1 feature images from all natural shares and then executes the XOR operation with share S.to obtain the recovered image, as shown in Fig. 2(b). The module which is the core module of the feature extraction process is applicable to printed and digital images simultaneously. Each module in Fig. 2 is described in the following sections.



4. THE PROPOSED ALGORITHMS

4.1. Feature Extraction Process

This section first describes the feature extraction module that extracts feature images from the natural shares. Then, the image preparation and the pixel-swapping modules are introduced for processing printed images.

4.1.1. The Feature Extraction Module

Feature extraction involves simplifying the amount of resources required to describe a large set of data accurately. When performing analysis of complex data one of the major problems stems from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory and computation power or a classification algorithm which over-fits the training sample and generalizes poorly to new samples. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy.

Best results are achieved when an expert constructs a set of application-dependent features. Nevertheless, if no such expert knowledge is available general dimensionality reduction techniques may help.

Assume that the size of the natural shares and the secret image are w .h pixels and that each natural share is divided into a number of b .b pixel blocks before feature extraction starts. We define the notations as follows:

- b represents the block size, b .even.
- N denotes a natural share.
- .*x, y*.denotes the coordinates of pixels in the natural shares and the secret image, 1 .*x* .w, 1 .*y* .h.
- .*x*1, *y*1.represents the coordinates of the left-top pixel in each block.
- *px,y* ϕ denotes the value of color ϕ, ϕ._R,G,B.for pixel .*x, y*.in natural share N, 0 .*px,y* ϕ .255.
- Pixel value H*x,y* is the sum of RGB color values of pixel .*x, y*.in natural share N and H*x,y*_*px,y R*.*px,y G* .*px,y B* . (1)
- M represents the median of all pixel values (H*x*1,*y*1, . . . ,H*xb,yb*) in a block of N.
- ***F*** is the feature matrix of N, the element *f x,y* .***F*** denotes the feature value of pixel .*x, y*_. If the feature value *f x,y* is 0, the feature of pixel .*x, y*.in N is defined as black.

If *f x,y* is 1 the feature of pixel .*x, y*.in N is defined as white.

As Fig. 3 shows, the feature extraction module consists of three processes—binarization, stabilization, and chaos processes. First, a binary feature matrix is extracted from natural image N via the binarization process. Then, the stabilization

balances the occurrence frequency of values 1 and 0

in the matrix. Finally, the chaos process scatters the clustered feature values in the matrix.

In the binarization process, the binary feature value of a pixel can be determined by a simple threshold function *F* with a set threshold. To obtain an approximate appearance probability for binary values 0 and 1, the median value M of pixels in the same block is an obvious selection as the threshold. Hence, for each block, the extraction function of

pixel .*x, y*.of N is defined as follows:

f x,y .*F* .H*x,y*_._1, H*x,y* . *M*, 0, otherwise. (2)

The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. The number of unbalanced black pixels Qs can be calculated as follows:

Q_s

$x_1 X x_b$

$y_1 Y y_b$

$f_{x,y}\ b_2$

2 . (3)

In the process, there are Qs pixels in which *f x,y* .1 is randomly selected and then the value of these pixels is set to 0. The process ensures that the number of black and white pixels in each block is equal.

In a natural image, pixels with the same or approximately the same values may cluster together in a continuous region.These clustered pixels have the same feature value; hence it will lead to the feature image and to the generated share revealing some textures of the natural image in the subsequent

encryption process. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share.

3 . (4)

Chaos is a kind of behavior about nonlinear dynamics law control. This paper adopts Logistic-mapping method to generate chaotic sequence:

$$a_{k+1} = \mu \cdot a_k \cdot (1 - a_k), k = 0,1,2,\cdots$$

The value traverses in the interval [0, 1], and μ is a control parameter or a bifurcation parameter. When

3.5699456…< u <= 4 , the logistic map works in chaotic state. The data stream gene- rated is disordered, and it's similar to random noise. The new binary sequence, which is the binarization of acquired chaotic sequence, has two main functions in this paper.

1. It is used to the encryption of text data information, which can enhance the security of the steganography.
2. It is used to stimulate the binary data stream, which can facilitate the process of various experiments.

Messy system is a dynamical system whose behavior changes with time. These changes are very sensitive to the initial conditions. This sensitivity manifests changes as an exponential growth of perturbations in the initial conditions. Thus, the behavior of messy system appears to be random, though they are deterministic. The dynamic changes of this system are completely defined by their initial conditions without any random elements. Therefore, the watermark is generated through messy system using the reference color plane as initial condition. Thereby, the watermark is generated dynamically. A general messy system is defined by the following equation

$$x_{n+1} = f(x_n)$$

Where f(*) refers the iterative, non linear function. It iteratively produces the values for initial value. It is known as messy sequence. The iteration will be stopped, when the parameters in f(*) satisfy a certain requirements for messy status. Once the sequence reached the messy status, it can be used to generate the watermark. In the proposed system, a hybrid optical bi stable messy system [23] is used which is defined by

$$f(x_n) = 4\sin^2(x_n - 2.5)$$

The watermark is generated through messy system by using prominent pixel values of reference color plane of the image as seed. Where, s(k) refers the pixel values of reference color plane of the image. a, band c are predefined constants and I refers embedding depth. The position information (pas) and secret key (key) is also used in the initial condition. The messy sequence is generated by substituting c_seg (k, 0) value for Xn in Eqn.2.For the kth pixel the sequence is referred as c_seq (k, i), i=l, 2, 3 ... 1. The reasonable number of iteration (I) is performed for the □ pixel to attain the messy status. This sequence contains

Algorithm1. *Feature Extraction Algorithm (FE)*

Floating numbers that is converted in to binary sequence in the proposed scheme

Algorithm FE( )

Input N,b,P_{noise}

Output:F

1. Divide N into blocks with b* b pixels.
2. For each block repeat Step 3
3. $\forall\ x_1 \le x \le x_b$, $y_1 \le y \le y_b$, calculate $H^{x,y}$ by Eq.(1)
4. Calculate M
5. $\forall\ x_1 \le x \le x_b$, $y_1 \le y \le y_b$, determine $f^{x,y}$ by Eq.(2)
6. Calculate Q_s by Eqn.(3)
7. Randomly select Q_s pixels where $f^{x,y}$ and $H^{x,y} = M$, let $f^{xy} \leftarrow 0$
8. Calculate Q_s by Eq.(4)
9. Randomly select Qs candidate pixels where $f^{xy} = 1$
10. Randomly select Qs candidate pixels where $f^{xy} = 0$
11. After all values of f that were selected in steps 9 and 10.
12. Output **F**

250	200	200	200
185	200	200	160
185	60	90	185
110	80	120	190

(a)

1	1	1	1
0	1	1	0
1	0	0	0
0	0	0	1

(b)

0	1	1	0
0	0	0	1
1	1	1	0
1	0	0	1

(c)

Fig4. *An example of the feature extraction process: (a) pixel values in a 4 x 4 block, (b) the resultant feature matrix in the stabilization process, (c) the resultant matrix in the feature extraction process.*

Qs 10 8 2, and two feature values at coordinates (1, 2), (1, 3), and (4, 3) must be set to 0. The resultant matrix in Step 7 is shown in Fig. 4(b). In this matrix, the feature values 0 and 1 are balanced. However, the extracted features remain clustered together; for example, coordinates (1, 1), (2, 1), (3, 1), (4, 1), (2, 2), and (3, 2) have the same feature value. Finally, by Eq. (4), there are Qc 4 2 2 0. 5 4 coordinates with feature value 1 (0) that must be altered to 0 (1). The resultant matrix in Steps 9–11 is shown in Fig. 4(c), with the altered feature values underlined. In this matrix, the clustering has been reduced. The feature matrix has the following properties:

Property1. The values 0 and 1 in the extracted binary feature matrix have the same appearance probability (i.e., 0.5 for each).

Proof. This property can be achieved by the stabilization process (i.e., Steps 6 and 7 in Algorithm FE).

Property2. The feature matrix depends on the contents of the corresponding natural image rather than the secret images. Property 2 indicates an important feature; that is, no one can decrypt the secret from the natural shares.

4.1.2. The Image Preparation and Pixel Swapping Processes

The image preparation and pixel swapping processes are used for preprocessing printed images and for post-processing the feature matrices that are extracted from the printed images. The suggested flow of the image preparation process is shown in Fig. 5. In the first step, the contents of the printed. The printed images were selected for sharing secret images, but the contents of the printed images must be acquired by computational devices and then be transformed into digital data.

(a) (b)

Fig. 6. *An example of the image preparation process: (a) a hand-painted picture (3264 x 2448 pixels) was captured by the digital camera on the iPhone 4S, (b) the resultant picture (512 x 512 pixels).*

Images can be acquired by popular electronic devices, such as digital scanners and digital cameras. To The next step is to crop the extra images. Finally, the images are resized so they have the same dimensions as the natural shares reduce the difference in the content of the acquired images between the encryption and decryption processes, the type of the acquisition devices and the parameter settings (e.g., resolution, image size) of the devices should be the same or similar in both processes. An example of the image preparation process is illustrated in Fig. 6. The hand-painted picture is drawn on A4 paper. First, the picture is captured using a popular smart phone, Apple iPhone 4, as shown in Fig. 6(a). The picture then is processed using the Paint application in Microsoft Windows 7.

Eventually, the picture is cropped and resized as a rectangular image as shown in Fig. 6(b). The resultant picture is used in the experiments in the subsequent section. Because of the distortions introduced into the acquired digital images during the image preparation process, different distortions are caused by each the encryption process and the decryption process. In other words, the acquired digital images in the encryption and decryption phases are not the same. These distortions result in noise that appears in the recovered images. When a large amount of noise clusters together, the image is severely disrupted, which may makes it impossible for the naked eye to identify it. The pixels-wapping process is used to cope with this problem. After the feature extraction process, a pixel-swapping module is applied to randomize the original spatial correlation of pixels in a printed image. The module pseudo-randomly exchanges the feature values of a pair of coordinates in a feature matrix. The permuted pixel sequence is determined by the random number generator. After the process, the distortions that were introduced in the image preparation process were spread in a feature matrix, and the noise also is distribute in the recovered image rather than clustered together. If the noise is distributed uniformly, the human visual system has a higher probability of recognizing the recovered image. In other words, the pixels-wapping module promotes tolerance of the image distortion caused by the image preparation process.

4.2. Encryption/Decryption Algorithms

The proposed (*n, n*)-NVSS scheme can encipher a true-color secret image by *n* . 1 innocuous natural shares and one noise like share. For one image, we denote a bit with the same weighted value in the same color as a bit plane; then a true color secret image has 24 bit-planes. Thus, the feature images and the noise-like share also are extended to 24 bit-planes. Each bit-plane of a feature image consists of a binary feature matrix that corresponds to the same bit-plane as the secret image. Before encryption (resp. decrypt) of each bit-plane of the secret image, the proposed algorithm first extracts *n*.1 feature matrices from *n* . 1 natural shares. Then the bit-plane of the secret image (resp. noise-like share) and *n* . 1 feature matrices execute the XOR operation (denoted by _.to obtain the bit-plane of the share image (resp. recovered image). Therefore, to encrypt (resp. decrypt) a true-color secret image, the encryption (resp. decryption) procedure must be performed iteratively on the 24 bit-planes. The notations used in the NVSS encryption/decryption process are defined as follows:

- ϕ denotes a color plane of an image, ϕ, R, G, B.
- S is the input image; Sϕ denotes an element of S in color plane ϕ.
- S is the output image; Sϕ denotes an element of S in color-plane ϕ.
- FIα denotes a feature image of natural share Nα.
- FIα,ϕ denotes an element of feature images in color-plane ϕ.

- $px,y\ \alpha,\phi$ denotes the pixel value of FIα,ϕ at coordinates $x, y\_$, 0 .$px,y,\ \alpha,\phi$ .255.
- ρ is the seed of the random number generator G.
- t is the amount of pixel swapping for a feature image of a printed image.

Algorithm 2 lists the encryption/decryption algorithms. The input natural shares (N1, . . .,N*n*.1.of the scheme include np printed images and nd digital images (n_p 0, n_d 0, n_p . n_d 1, and *n*. n_p . n_d . 1. The np printed images must be processed and transformed into digital form in the image preparation process. All input images are 24-bit/pixel truecolor images. Step 1 initializes random number generator G by seed ρ. Function G is used for the feature extraction and pixels-wapping processes. The encryption and decryption processes use the same seed ρ to generate an identical pseudorandom sequence. Step 3 initializes all feature images; that is, resets all pixel values $px,y\alpha,\phi$ in all feature images FIα. Steps 4–6 extract one feature image with a 24-bit depth per pixel from each natural share. Step 5 extracts a binary feature matrix from a natural share by calling algorithm FE. Step 6 adds the extracted matrix to corresponding bit and color planes of a feature image. Steps 8–11 perform the pixel-swapping process for each feature image extracted from the printed images. For each feature image, the pixel-swapping process randomly selects a pair of pixels in a feature image in Steps 9 and 10, and then swaps the values of two pixels in Step 11. Step 12 stacks input image S and feature images FI1,…, Fi*n*.1 by applying the XOR operation in each color plane. Finally, the resultant image S is the output in Step 13. The pseudo code of the algorithm is for true-color secret images; however it is also applicable for 8-bit gray and binary images. In the case of an encryption/decryption gray (binary) secret image, the algorithm extracts an 8-bit (1-bit) feature image for each natural image to fit the information quantity of the secret image. There are two main loops in the algorithm: Steps 4–6 and Steps 8–11. The time complexity of algorithm FE is O.hw_. The time complexity of Step 4–6 is O.*n*cdhw, where cd represents the color depth of a pixel. The value of cd depends on the color depth of the secret image. For example, if the secret image is with 24-bit/pixel color depth, the value of cd is 24. The value of cd is 8, while the secret image is a gray image with 8-bit gray levels. The time complexity of Steps 8–11 is O.npthw_. Hence, the complexity of the encryption/decryption algorithm is *max* O.*n*cdhw_,O.npthw. The algorithm in Algorithm II can be used for the encryption and decryption phases by setting various parameters as follows:

Encryption: Input images include *n* .1 natural shares and one secret image. The output image is a noise-like share. Decryption: Input images include *n*.1 natural shares and one noise-like share. The output image is a recovered image. The proposed encryption algorithm has the properties discussed below.

Property3. The amount of information required for the generated share is the same as for the secret image.

Proof. In the encryption process of the algorithm, one binary feature value must be extracted from one natural share to share 1 bit of a secret pixel. Each pixel in the generated share is yielded by XOR-ing the corresponding secret pixel and *n*.1 binary feature values that were extracted from *n* . 1 natural shares. Therefore, the generated share has the same amount of information as the secret image.

Property3 shows that the generated share in the proposed (*n, n*)-NVSS scheme is free of pixel expansion.

Property4. Pixel values in a feature image are distributed uniformly over [0, 255].

Proof. As proved in Property 1, values 0 and 1 share the same appearance probability in a feature bit. In Step 6 of the NVSS.

4.3. Hide the Noise-Like Share

In this section, steganography techniques are introduced to hide or conceal the noise-like share and further reduce intercepted risk for the share during the transmission phase. In the proposed NVSS scheme, a dealer can hide the generated share by using existing steganography. The amount of

information that can be hidden in a cover image is limited to an extent and depends on the hiding method that we will be using for the purpose. To embed the generated share in a cover image, the dimension of the cover image must be larger than that of the secret image. Cover image must be atleast triple the size of the secret image. If the share can be hidden in the cover image and then can be retrieved totally, the secret image can be recovered without distortion.

5. EXPERIMENTS

In this section, we have performed two experiments to evaluate the performance of the proposed NVSS scheme.

Fig8. *The natural shares (N1, N2, and N3) in a (4, 4)-NVSS scheme: (a) N1, (b) N2, (c) N3.*

Fig9. *Experimental results of Experiment-I: (a) share S, (b) S exor FI1, (c) S exor FI1 exor FI2, (d) S exor FI1 exor FI3, (e) S exor FI2 exor FI3, (f) recovered image of SE1 (S FI1 exor FI2 exor FI3.)*

4.1. Experiment I

This subsection demonstrates the performance of the proposed NVSS scheme in the case of a .4, 4_-NVSS scheme. Fig. 8 shows us three natural shares in the experiments. The secret image SE1 is the well-known picture—"Lena" (as shown in Fig. 9(f)). All natural shares are taken from travel photos of tourists. These images dimensions are 512 .512 pixels and all are in true color format. Parameters b and P*noise* are set to 8 and 0.5, respectively. Fig. 9(a) shows share S yielded by the .4, 4_-NVSS scheme. The appearance of S consists of a large amount of random pixels and the textures are concealed, which indicates that the algorithm is very efficient at eliminating textures in the share Fig. 9(b) to Fig. 9(f) provide examples of reconstructed.

Images obtained by stacking noise-like share S and the feature images (denoted as FI. Fig. 9(f) is the perfectly recovered image decrypted by stacking share S and all feature images (i.e., FI1, FI2, and FI3) All the other images (i.e., Fig. 9(b) to Fig. 9(e)) cannot reveal any texture related to the natural shares or the secret image because one or more of the natural shares is missing. Fig. 10 is the graphical representation showing the statistical results on the distribution of pixel values in share S and secret image (SE1, Lena). The distributions in SE1 in the red, green, and blue color planes are denoted as Secret (R), Secret (G), and Secret (B). Fig. 10 shows us that the distribution in S (denoted as Share in Fig. 10, in each color plane is very random; it is completely different from the distribution in SE1. Hence, it is difficult to obtain any information related to SE1 from share S. The distribution in share S also agrees with Property 5.

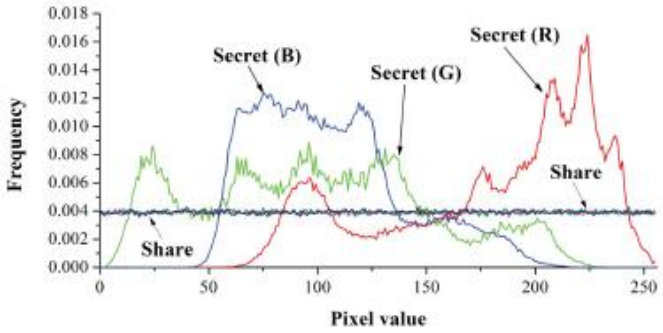


Fig. 10. *The distribution of pixel value in share S and secret image SE1.*

4.2. Experiment II

This experiment will evaluate the performance of the proposed NVSS scheme for sharing color and binary secret images by diverse shares. The shares used in the.5, 5-NVSS scheme includes one hand-painted picture and three digital images. The color secret image and digital images are the same as those used in Experiment I. The hand-painted picture is drawn on A4 paper, as shown in Fig. 6(a).

The picture is processed by the image preparation process to obtain two digitized shares, one for the encryption process and one for the decryption process. The digitized share for the encryption process is captured by a digital camera—Canon 650D, as shown in Fig. 10(a). Another digitized share is captured by the digital camera on a smart phone, iPhone4, as shown in Fig. 10(b).

After the image preparation process, all images in the experiments are 512*512 pixels. Parameters b and Pnoise for all digital shares are set to 8 and 0.5, respectively. Parameter b for the printed share is set to 256. Fig. 11(c) shows the difference between Fig. 11(a) and Fig. 11(b). The difference can be evaluated by the quantitative metric—PSNR (the peak signal to noise ratio). The PSNR value between Fig. 11(a) and Fig. 11(b) is only 19.74 dB. The low PSNR means that high distortions are introduced into the digitized share that will be used in the decryption phase.

Fig11. *Experimental results of Experiment-II: (a) the digitalized share that is captured by Canon 650D digital camera, (b) the digitalized share that is captured by iPhone 4, (c) difference between Fig. 11(a) and Fig. 11(b), (d) recovered image of SE1 (PSNR = 12.12 dB), (e) binary secret image (SE2, (f) recovered image of SE2 (contrast = 60.64%).*

The distortion is introduced by various devices in capturing the hand-painted share during the encryption/ decryption phases.

Fig. 11(d) and Fig. 11(f) illustrate the recovered image of the NVSS scheme for sharing color image SE1 and binary image SE2 (as shown in Fig. 11(e)).

Although applying a printed share for the image sharing, noise will be introduced to the recovered image; the display quality of the recovered image remains clear enough to be recognized by the naked eye. The result is that the proposed NVSS scheme can use printed images as sharing images. This outcome is significant and has not been presented in previous research.

All the secret images are binary and have the same cipher text—"NO SECRET Here". Parameters b and P*noise* are set to 8 and 0.5, respectively. Fig. 12(a), (b), and (c) are the recovered images for three images with various dimensions: 128*128, 256 * 256, and 512*512 pixels. When the amount of information of the share increases, the contrast of the recovered images remains at an acceptable level. The secret image used in this experiment is a binary image of size 256*256 pixels. Fig. 12 (d) to Fig. 12(f) demonstrate the implementation results of a noise and the recovered image in the .4, 4_-NVSS scheme.

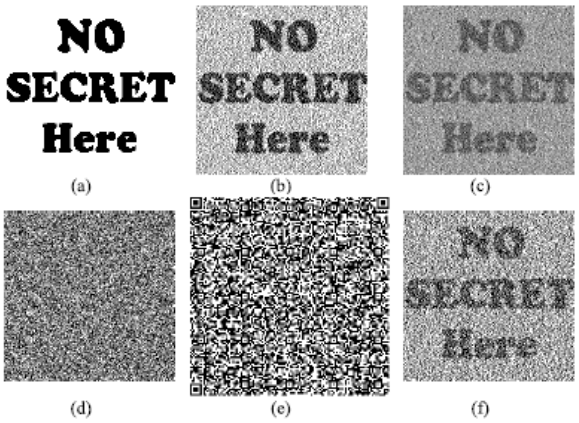


Fig12. *Experimental results of Experiment II: (a) recovered image (128 *128 pixels, 96 dpi, contrast =100%), (b) recovered image (256 *256 pixels, 192 dpi, contrast = 50.11%), (c) recovered image (512 * 512 pixels, 384 dpi, contrast = 22.65%), (d) noise share (256 * 256 pixels, 192 dpi), (e) the corresponding QR code (version 25, the error correction level: L) of Fig. 12 (d), (f) recovered image (256 * 256 pixels, 192 dpi, contrast = 31.32%), which adopts the QR code in Fig. 12(e) as the stego-share.*

6. CONCLUSION

The paper proposes a VSS scheme, (*n*,*n*)-NVSS scheme, that shares a digital image using diverse image media. The media that include *n*.1 randomly chosen images are unaltered in the encryption phase. Therefore, they are completely innocuous. Regardless of the number of participants *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness and highest level of security, both for shares and for participants.

This study provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce hand-printed images for image sharing schemes. Third, this study proposes a useful concept and method for using unaltered images as shares in a VSS scheme.

ACKNOWLEDGMENT

Hereby, the authors appreciate the anonymous reviewers for their valuable comments.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," *Opt. Commun.*, vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[3] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[4] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," *IEEE Trans. Image Process.*, vol. 22, no. 10, pp. 3830–3841, Oct. 2013.

[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[6] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 21, no. 5, pp. 879–898, Aug. 2007.

[7] 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, Feb. 2012.

[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[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, Jan. 2011.

[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[12] 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, Nov. 2011.

[13] LEE AND CHIU: DIGITAL IMAGE SHARING BY DIVERSE IMAGE MEDIA "IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014"