International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

DIGITAL IMAGE SHARING USING NVSS

RAJESHREE KALE, SNEHA WALKE, POOJA MESHRAM, TRIVENI DONGRE

Department Of Computer Engineering, Dhole Patil College Of Engineering, Maharashtra, India

---

Abstract - We have propose a VSS scheme, which is called as the natural image–based VSS scheme (NVSS scheme), to reduce the risk during the transmission phase. Conventional VSS schemes use a unity such as 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 digital images, printed images, hand-painted pictures. 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 and . Instead of altering the contents of the natural images, the proposed approach extracts features from each natural share.These unaltered natural shares are totally innocuous, and thus greatly reduces 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 during the transmission phase.

The NVSS scheme uses diverse media as a carrier; hence it has many possible views for sharing secret images. To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk.

Key Words: Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk. for solving the transmission risk problem for the VSS schemes.

1. INTRODUCTION:

A natural-image-based secret image sharing scheme (NVSS) that can share a color secret image over n - 1 arbitrary natural images and one noise-like share image. Instead of altering the contents of the natural images, the encryption process extracts feature images from each natural image. In order to protect the secret image from transmission phase. (n, n) - NVSS scheme shared secret image over n-1 natural share. The natural shares will be digital image and printed image. By extracting the features of natural shares we can prepare noise-like share. After that encryption carried out with noise-like share and secret image. We have Propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. In this paper Initially Digital image and Printed image have been used as Natural Shares for performing Feature Extraction process .Here extracted features, secret image will be encrypted by (n, n) - NVSS scheme where process carried by (n-1) natural shares. This Encrypted result will be hided using Share-Hiding

Algorithm will generated the QR code. In the Recovering of the secret image will be done by Share Extraction Algorithm and also decryption algorithm. Finallywe get the secret image with all pixels has been obtained. This proposed possible ways to hide the noise like share to reduce the transmission risk problem for the share.

Encryption is used to securely transmit data within two networks.Encryption has its two different keys. Each type of data has its own features, different methods should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. A block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm is called as Blowfish. We divide the original image into blocks, which were sorted into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. Encryption is the process of transforming the information to insure its security. With the large growth of computer networks, a large amount of digital data is being exchanged over different types of networks. Therefore , different security techniques have been used to provide the protection. The security of digital images has gained attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another image that is difficult to understand ie it converts into another form which is encoded. On the other hand, image decryption retrieves the original image from the encrypted one. There are different image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

1.1 Module Description:

Image Preprocessing
In our Proposed Method Printed image will be preprocessed by cropping the input image. Cropping of image is performed manually and stored for further processing. Then we resize the cropped image with predicted size.

Feature Extraction

Feature Extraction is carried out by Binarization process . It is performed by calculation which is taken with respect to the median value of the natural share. With the binarization result comes out ie. it is the stabilization process has been done. The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. This process ensures that the number of black and white pixels in each block is equal. These clustered pixels have the same feature value because clistering has a group of similar classes. The chaos is th process which is used to eliminate the texture that may appear on the extracted feature images and the generated share. The original feature matrix will be disordered by adding noise in the matrix.

Encryption:

Before starting to Encryption process pixels-swapping for printed image share performed which promotes tolerance of the image distortion caused by the image preparation process. The proposed NVSS scheme can encipher a true color secret image by n-1 innocuous natural shares and one noise like share. Input images include n-1 natural shares and one secret image. The output image which we get is a noise-like share. Finally XOR operation is performed for each color plane with the secret image. Encryption uses a key to encrypt a image .And Decryptor uses a same key to decrypt.

Data Hiding:

In this section Quick-Response Code (QR code) techniques are introduced to hide the noise-like share and further reduce intercepted risk for the share during the transmission phase. The code is printed on physical material and can be read and decoded by various devices, such as barcode readers and smart phones. It is suitable for use as a carrier of secret communications. The string can be encoded to the QR code by QR code generators.

Decryption:
By repeating the reversal process of encryption process to predict the secret image. Again feature extraction and pixel swapping performed to predict the secret image.

Encryptor Module:
This module has 4 sub modules:

- Rescaling Module: Input - All 3 images 1 secret image,2 natural images. Output - 3 images rescaled.

- Feature Extraction Module: Input - 2 natural images. Output – 2 feature matrices.

- VSSS Encryptor : Input - 1 secret image,2 feature matrices. Output – 1 noise Image.

- QR Generator : Input - 1 noise image, 1 Dummy string. Output – 1 qr Image.

Decryptor Module:
This module has 4 sub modules:

- Rescaling Module: Input - 2 natural images. Output - 2 images rescaled.

- Noise Extraction Module : Input - 1 qr image. Output - 1 noise images.

- Feature Extraction Module: Input - 2 natural images. Output – 2 feature matrices.

- VSSS Decryptor : Input - 1 noise image,2 feature matrices. Output – 1 secret Image.

2. EXISTING TECHNIQUE:-

Visual Cryptography (VC) is a technique that encrypts a secret image into n shares, with each participant holding one or more shares. Stacking the n shares reveals the secret image and it can be recognized directly by the human visual system[1]. In cryptography text is send in encrypted format for sending message sender use one key for encryption and for decryption same or different key is used. Secret images can be of various types: images, handwritten documents, photographs, 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. There are two drawbacks . Attacker can easily predict key by some combinations. If lack of security problem if attacker get key then he can access message[2]

The Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme provided some effective solutions to cope with the management issue. In Visual Secret Shearing noisy image get created[8]. As directly contents are not visible. Noisy image is sent and receiver

acquire natural image from it.But it is much better than a visual cryptography. The proposed NVSS Scheme can share a digital secret image over n-1 arbitrary natural images (hereafter called natural shares) and one share. Instead of altering the contents of the natural images, the proposed approach extracts features from each natural share. These unaltered natural shares are totally innocuous, thus greatly reducing the interception probability of these shares.Drawbacks of these are whole image is noisy attacker can predict that, shearing is there. And he is smart enough that he apply different techniques for accessing it[7].

Steganography is the technique of concealing information and making the communication invisible. The hidden information and its carrier can be protected. Steganography has been used to hide digital shares in VSS schemes. Theshares in VSS schemes are embedded in cover images to create stego-images. Although the shares are concealed totally 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. In steganography text is hidden inside image. And image is send. This is better than Cryptography. As Image is there, text is not directly visible.If attacker get the image then there is direct access of data so this is also not the better technology[].

Recently, Chiu et al. tried to share a secret image via natural images . This was a 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, printed images cannot be used for sharing images in the previous scheme like visual cryptography,segnography. So far, sharing visual secret image via unaltered printed media remains an open problem. In this study, we make an extension of the previous work in to promote its practicability and explore the possibility for adopting the unaltered printed media as shares.

We use efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. The proposed algorithms are applicable to digital and printed media. The feasible ways to hide the generated share they 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.

2. THE PROPOSED SCHEME

2.1Background

In cryptography, the one-time pad (OTP), which was proven to be impossible to break only if we use is correctly, It 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 aencrypted form of a original 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. We can use same as well as different keys for encryption and decryption.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 such as receiver and sender who are involved 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.

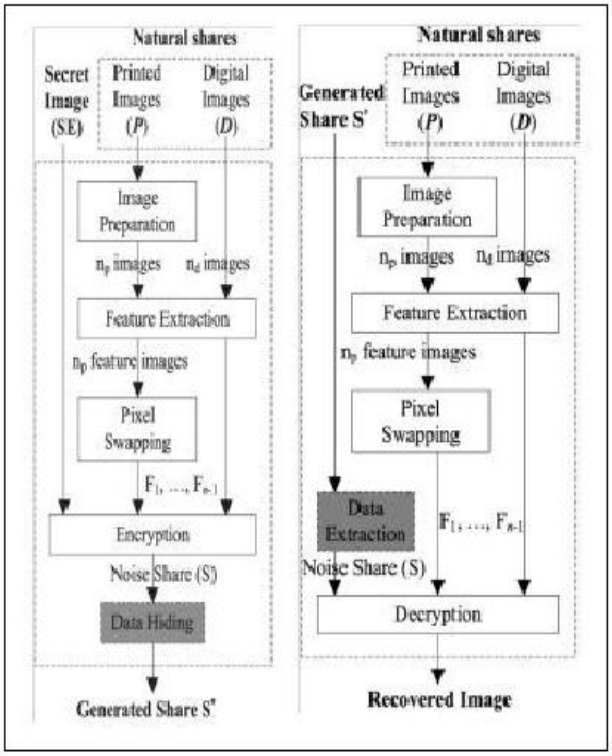


Fig -1:BLOCK DIAGRAM

The Proposed (n,n)NVSS Scheme

As Fig. 1.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 n digital images (denoted as *D*), np- 0, nd - 0, np -nd -1 and n -np -nd -1. The feature images (F1,…, Fn-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,…, Fn-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. 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.

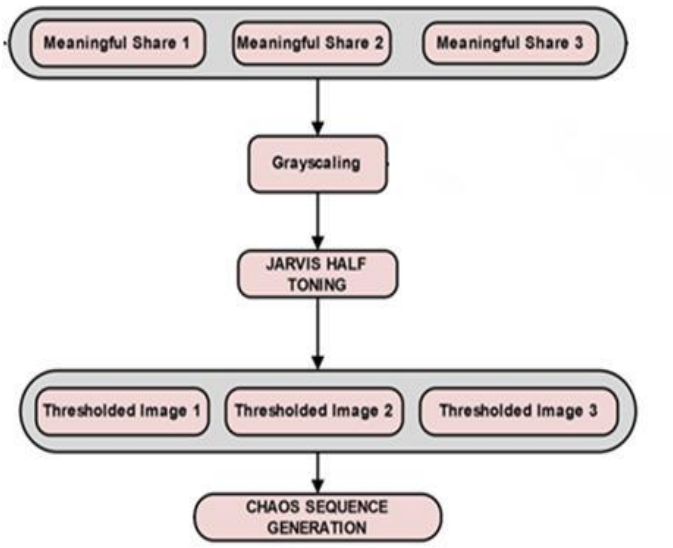


Fig -2: FEATURE EXTRACTION PROCESS

2.2 THE PROPOSED ALGORITHMS

Feature Extraction Process
Feature Extraction Process 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.

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 are 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.
- x1, *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. 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 .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.In the process, there are Qs pixels in which *one* 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 .

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 generated 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)*

1. Divide N into blocks with b* b pixels.
2. For each block repeat Step 3
3. x1 ≤ x ≤ xb , y1 ≤ y ≤ yb , calculate Hx,y by Eq.(1)
4. Calculate M
5. x1 ≤ x ≤ xb , y1 ≤ y ≤ yb , determine fx,y by Eq.(2)
6. Calculate Qs by Eqn.(3)
7. Randomly select Qs pixels where fx,y and Hx,y = M , let fxy 0
8. Calculate Qs by Eq.(4)
9. Randomly select Qs candidate pixels where fxy =1
10. Randomly select Qs candidate pixels where fxy =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)

Fig 3.
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.

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. 3(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 .42_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. 3(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.

2.3 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. 4. 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.

Fig 4
Fig. 4. 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 taken by popular electronic devices, such as digital cameras. 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 of the devices should be the same or similar in both processes. An example of the image preparation process is illustrated in Fig. . The hand-painted picture is drawn on A4 paper. First, the picture is captured using a popular smart phone 4(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. 4(b). 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 is impossible for the naked eye to identify it. The pixelswapping process is used to cope with this problem. Pixel swapping process is used to swap. After the feature extraction process, a pixelswapping 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.

2.4 . 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, a bit with the same weighted value in the same color is denoted 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
- FI*α* denotes a feature image of natural share N*α*.
- FI*α,*ϕ denotes an element of feature images in color-plane ϕ.
- *px,y α,*ϕ denotes the pixel value of FI*α,*ϕ at coordinates *x, y*_, 0 .*px,y, α,*ϕ .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.

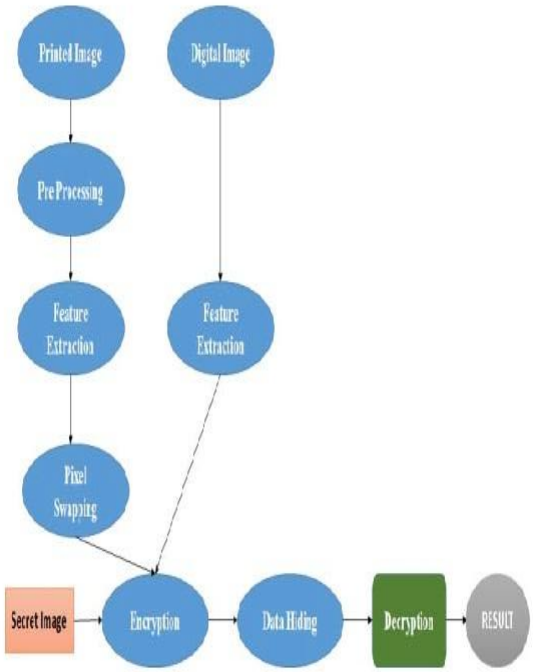
Algorithm 2 lists the encryption/decryption algorithms. The input natural shares (N1, . . .,N*n*-1).of the scheme include np printed images and nd digital images (np . 0, nd . 0, np - nd .-1, and *n*.-np - nd - 1. The np printed images must be processed and transformed into digital form in the image 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,yα,*ϕ in all feature images FI*α*. 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; hence it is also applicable for 8-bit gray images and binary images. In the case of an encryption and 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 8–11The 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 amount of information required for the generated share is the same as for the secret image. 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.

2.5 Hide the Noise-Like Share

In this we hide the noise like share ,in this section, steganography techniques are introduced to hide 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 bigger ie. 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.

3.RESULTS

We have implemented NVSS scheme In our proposed system (n, n) . In NVSS scheme both printed image and digital image have been taken into account to create the noise and this noise image is share.This natural image need to be extracted feature for further process. With the feature image and secret image can be perform in encryption process. By applying (n, n)- NVSS scheme developed encrypted image or (n-1) natural share.The Feature extraction has been performed for two natural Shares. So as the natural share's pixels are more efficiently compressed. This extracted features are encrypted with Secret Image. This process is performed by (n, n) – NVSS scheme. Then the encrypted image will be hided using by share hiding algorithm. Encryption process performed with the QR code technology. QR code is a two-dimensional code.The QR Code system has become popular outside the automotive industry due to its fast readability. QR code is greater storage capacity compared to standard UPC barcodes. The transmission risk is conventional VSS schemes are increases in every time and rapidly. On the contrary, regardless of the increasing number of shares, the proposed NVSS scheme are always requires only one generated share. In decryption process is share extraction algorithm and perform decryption algorithm . It applied to recover the Secret image.



4. CONCLUSIONS

In this paper we have proposes a VSS scheme, (n,n)-NVSS scheme,that can share a digital image using diverse image media. Themedia that are include n-1 randomly chosen images and unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of n increases, the NVSS scheme uses only for the one noise share . This one noise share for sharing the secret image. Compared with the existing VSS schemes. The propose NVSS scheme can be effectively reduce transmission risk and provide the highest level uses for shares and for participants. This study provided the four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we are successfully introduce in the hand-printed images for images-haring schemes. Third, this study proposes a useful in the concept and method for using unaltered images as shares in a VSS scheme. Last is, we develop a method and store the noise share as the QR code.

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]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.

[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]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.