Digital Image Sharing by Diverse Image Media

Prof.Shubhangi Dixit
Department of Information Technology Engineering
PVGCOET, Pune, Maharashtra, India

Shamal Jamdade
Department of Information Technology Engineering
PVGCOET, Pune, Maharashtra, India

Prajakta Borate
Department of Information Technology Engineering
PVGCOET, Pune, Maharashtra, India

Rashmi Kothawade
Department of Information Technology Engineering
PVGCOET, Pune, Maharashtra, India

Prachi Kelkar
Department of Information Technology Engineering
PVGCOET, Pune, Maharashtra, India

Abstract- In today's world, information is the most important part of any organization. The information is often shared between the organizations or transferred from person to person .Hence ,Information security plays a vital role in the field of communication .Hence ,there is need to protect the information that is being shared. Conventional visual sharing schemes (VSS) hides the secret in the noisy share hence it increases the interception risk . So ,to overcome this problem we use Natural-image-based VSS scheme(NVSS) where we share the secret image by various media to provide security to the secret image . The NVSS involves one digital secret image, n-arbitrary natural images[natural shares] and one carrier image. The natural images can be any photos or pictures in digital form. Using this natural images key is generated. By using this generated key and secret digital image, we create a noisy share. Steganography technique is used to hide noisy share into carrier image. The natural images are transmitted using different media. Hence we reduced the transmission risk. To provide security to natural shares digital watermarking is done.

Keywords – NVSS, VSS, Visual Cryptography, Digital watermarking

I. INTRODUCTION

Sharing a secret in computer aided environment has become important issue. To provide security to the secret image we use NVSS technique. In this technique n+2 images are used for secret sharing (n for natural images, one carrier image, one secret image). N natural images are distributed to participants. The key is required for encryption of secret image and is generated from n natural images. At receiver side anyone who holds fewer than n natural images cannot generate a key. Stacking n natural images reveals the key and we can decrypt the secret image. The motivation of NVSS scheme is to securely share secret images in non-computer aided environment.

Using conventional shares for secrete sharing does not satisfy the security requirement. The suffer from the two drawback first there is high transmission risk because of noise like shares hence There is risk of transmission failure, second as

the number of shares increases it becomes difficult to manage. This issue can be manage by the existing vss scheme. The shares contain noise like pixel. These shares can be detect as suspicious. these shares are embedded in another carrier image by the process called steagnography. However it can be detected by steagnoanalysis. We use vss scheme called as natural image based vss scheme to reduce the transmission risk. Conventional vss uses one carrier media whereas In proposed schema we use diverse media for sharing natural images and secret image. By applying diversity in media reduces interception risk and maintain the confidentiality and integrity of secret information. We also apply digital watermarking to natural shares to maintain integrity of images. In proposed NVSS scheme, we handle n natural images and two images one as carrier image and another one as secret image. Instead of changing the natural images extract features from natural images and generate the numeric key. Share these natural images using diverse media to enhance level of security. Noisy share of secret image is generated using key and hidden into carrier image to increase security level. In this paper we develop encryption, decryption and watermarking algorithm for NVSS scheme. The proposed algorithm is applicable to digital images. The proposed schema provides three level securities, manageability and reduces transmission risk.

II. EXISITING SYSTEM

A.Background-

In cryptography ,the OTP (one- time pad),which is prove impossible to break if used correctly ,it was developed by Gilbert Vernam in 1917.In which each bit or character from the plaintext is encrypted with the secret random key of same the length resulting into the cipher text .This cipher text was send to the receiver and then receiver decrypt the cipher text with the same key which sender has used to get the original message . Steganography is the technique of information hiding in order to conceal the existence of the information. The visual secret sharing scheme is similar to the OTP encryption system . In VSS scheme The cipher text and random key is treated as shares and given to two participants .The two participants can decrypt the cipher text to get the original message by applying the random key. We use the OTP technique and steganography to share digital visual secret .Here instead of generating the random key we take two natural shares or any natural images and generate the random key from this two natural images which is used to encrypt the secret image and generate the noise share and then this noisy share is hidden in another carrier image . This carrier image and the natural images is distributed in the participants .In decryption the key is generated from the natural shares and this key with the noise share is used to recover the original secret image. This scheme can be extended to the n natural images.

B. *NVSS scheme*

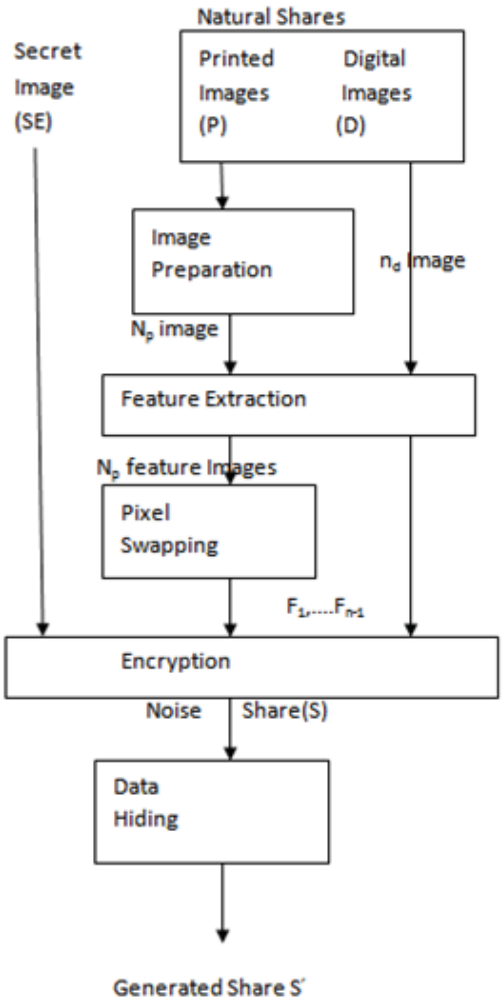

Fig.1(a)

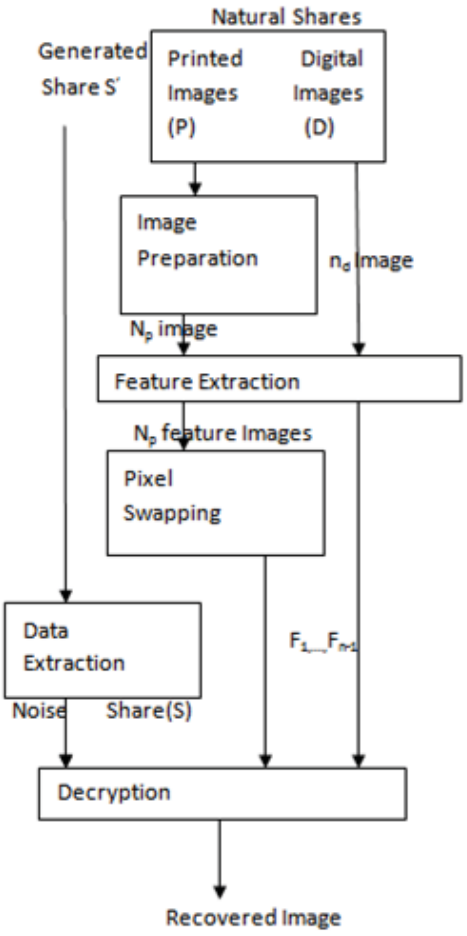

Fig.1(b)

Fig .1 shows the encryption and decryption process .It includes three phases :
Image Preparation, Feature Extraction and encryption. In image preparation phase preprocessing operations like binarization, stabilization are applied on image.

In feature extraction feature image is extracted from the natural images(n1,n2).The feature images (f1,f2)are combined to form one feature image. In the encryption phase , the feature image and the secret image execute the XOR operation to generate one noise-like share S ,this generated share S is concealed behind cover media by steganography technique. When all natural images and the carrier image is received by the receiver the decryption process is carried out .The featured image is extracted from natural image and XOR is performed to recover the secret image as shown in Fig.1 (b).

C. *Feature Extraction-*

Feature extraction process consists of three operations: Binarization , Stabilization and choas process .First the binary feature matrix is extracted from the natural images .In Binarization process, the binary value is determine by simple thresholding function(Ƒ) to obtain the approximate binary value 0 or 1 calculate the median.
So ,the extraction function of pixel(x,y)of N (natural image) can be define as:
$F_{x,y}=Ƒ(H_{x,y})=\{ 1, H_{x,y} \geq M ,$
0, otherwise.

Stabilization process balance the number of black and white pixels in the featured image .i.e It balances the occurrences of 0 and 1 in the feature image. The texture on the feature image is eliminated by using choas process and then generate the share .In this process noise is add to the feature matrix and it is disordered after the feature extraction process pixel swapping module is applied to the feature image .The random number generator is used to get the number and then simply exchange the feature value of the co-ordinate.

D. *Encryption and Decryption –*

Encryption :
In Encryption process XOR operation is performed between the secret image and the feature image to obtain the noisy share.
Decryption :
In Decryption process XOR is performed between the received share and feature image extracted from the natural images(natural shares).

C. *Hide the Noise-like share*

Steganography and Quick response code is used to hide the information or the share. The existing system uses the QR code to hide the information. QR code is the 2Dimensional code Which encodes the meaningful information .Encoding process is the two step process. first transform pixel on the share into binary values and second represent the values in decimal format. Today QRcode is widely used in commercial catalogs & flyers, in electronic media ,& everywhere. The ubiquitous nature of the QR code makes it suitable for use as a carrier of secret communications.

III.PROPOSED SYSTEM

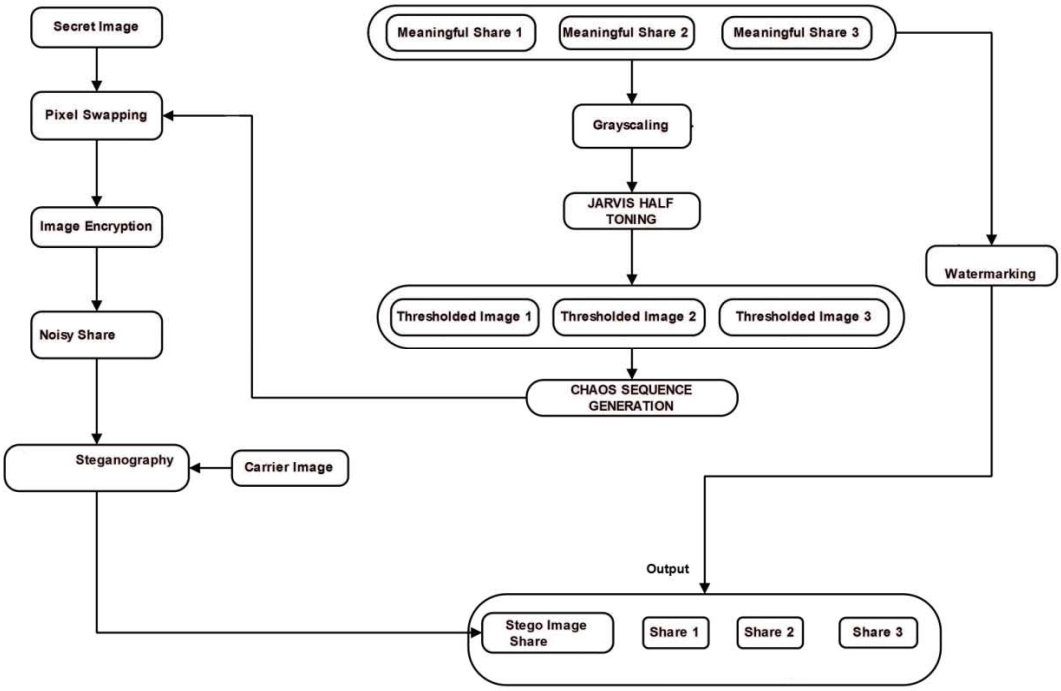

Fig.2

The above figure shows the proposed system of digital image sharing by diverse image media. In this system we generate the secret key for pixel swapping of secret key image. For key generation we use three natural images(meaningful shares). we can use 2 0r more natural images for key generation. For key generation image processing is done like (gray scaling and Jarvis half toning). In Jarvis half toning image thresholding is done. Using this threshold images key is generated. Using the secret key and hennonmap equation pixel swapping of the secret image is done and noisy share is generated. To provide more security we use Steganography. In Steganography the noisy share is hiding in the carrier image using LSB replacement. Then the stego image is send to the receiver. To provide security to the natural images alpha channel watermarking. In alpha channel watermarking the average of RGB is store in the alpha channel and at receiver side the receiver verifies the alpha channel value to check the integrity of the natural image (meaningful shares).

A.Image Pre-processing -

The image is considered as the Two-dimenssional array of the pixel.Each pixel representing the 32-bit entity of which 24-bits are used to store the RGB(Red,Green,Blue) components. The process includes pre-processing techniques such as loading of the natural shares, grayscaling, Jarvis halftoning. The algorithms are described in the following subsection.

1.Gray Scaling-

Converts the colourful natural images to grayscale images.color is a 24 bit integer (actually 32 but only 24 bits when a pixel is considered each 24bit is composed of individual 8 bits of Red green and blue hence in order to separate red, green and blue we need to mask this integer e.g. value color is 0x435A56 where 0x43 is red, 0x5A is green and 0x56 is blue now to separate blue we can LOGIC AND the col with 0xFF (i.e. eight 1's)

0x435A56 AND 0x0000FF ---------- 0x000056 – blue separated.

now to separate green we will first right shift the col by 8 so that green color comes down to LSB portion
0x435A56 >> 8 = 0x435A and now ANDing it with 0xFF will give us only green Component.
0x435A AND 0x00FF ---------- 0x005A - green separated.

ALGORITHM: Grayscale ( )
INPUT: N1(natural share)
OUTPUT: N1 (grayscaled image)

1. For each pixel repeat 2-4
2. b = col & 0xff;
   g = (col >> 8) & 0xff;
   r = (col >> 16) & 0xff;
3. gs = (r + g + b) / 3;
4. r = g = b = gs;
5. End of Loop
6. Store the graycale image.
7. Output
8. End

2.Thresholding-

Richard Howland Renger received a patent for his invention.Digital halftoing is the methodof converting the continuous tonned imageinto a black andwhite image such that when viewed by the human vision pattren createsa illusion ofcontinous gray shed.The input image is converted into a Jarvis halftoning image of same size using Jarvis error diffusion method i.e.converts the greyscaled image into the black and white pixels using Jarvis error diffusion technique. The equations are as follows for each pixel of
image[x][y].
1.image[y][x + 1] = ((7 / 16.) * error) + image[y][x + 1];
2. image[y + 1][x + 1] = ((1 / 16.) * error) + image[y + 1][x + 1];
3. image[y + 1][x] = ((5 / 16.) * error) + image[y + 1][x];
4. image[y + 1][x - 1] = ((3 / 16.) * error) + image[y + 1][x - 1];

ALGORITHM: Threshould ( )
INPUT: N1(natural share)
OUTPUT: N1 (threshould image)

1.call to function jarvis_halftoning.
2.For each pixel repeat step 3-4
3. gsTh1 = temp1[y][x] < 128 ? 0 : 255;
4. th1[y][x] = gsTh1
5. End of Loop
6. Store the threshould image.
7. Output
8. End

ALGORITHM: jarvis_halhtoning()

1.initialize threshold value Th.
2.for each pixel repeat steps 3-7
3. tempPixel = (image[y][x]>=T) ? 255 : 0;
   error = -tempPixel + image[y][x];
4. if((x+1)<w)
   image[y][x+1] = ((7/16.) * error) + image[y][x+1];
5. if((x+1)<w && (y+1)<h)

```
   image[y+1][x+1] = ((1/16.) * error) + image[y+1][x+1];
 6. if((y+1)<h)
    image[y+1][x] = ((5/16.) * error) + image[y+1][x];
  7. if((y+1)<h && (x-1)>=0)
     image[y+1][x-1] = ((3/16.) * error) + image[y+1][x-1];
  8.End.
```

B. Image Encryption-

1.key generation()

Numeric key is generated from the natural shares by XORing the black and white pixel.

ALGORITHM: Key_Generation ( )
INPUT: N1,N2,N3
OUTPUT: Key

1. Do for each image N1,N2,N3
2. For each pixel repeat 3-4
3. Calculate threshould value.
4. set the value to 0 or1.
5. End of Loop
6. KEY<- Calculate number of 0 and 1
perform XOR operation.
7. Store the watermark image in each natural
images alpha channel.
8. Output KEY
9. End

2.Encryption()

The secret image is encrypted using the key obtained from meaningful shares. This process includes the repositioning of the pixels of the secret image.For chaotic sequence, The use of Hennon-map equation is done.The two eqution are as follows:

$X_1 = 1 + y_0 - (\alpha * x_0 * x_0);$
$Y_1 = \beta * = x_0;$

ALGORITHM: Encryption ( )
INPUT: KEY,SECRET_SHARE
OUTPUT: S_SHARE

1. New_PIX <- Generate new pixel co-ordinates(x_1,y_1) using chaotic equations
2. Add Ascii value of Key to the new co-ordinate value.
3. SHARE <- Shuffle the co-ordinates(x_0,y_0) to(x_1,y_1)
4. Calculate LSB of the cover image
5. S_SHARE < - Replace the LSB bits of cover image with the bits noisy secret image.
6. Output S_SHARE
7. End

C.Steganography-

To improve the security of the share further we can make useof data hiding techniques like steganography. Cryptography and Steganography work very closely with each other to improve the security of the noisy share.

If we want to encode A (ACSII value 65 or a binary value (01000001) in the below given carrier file.

01011101 11010000 00011100 10101100
11100111 10000111 01101011 11100011

After Embedding
01011100 11010001 00011100 10101100
11100110 10000110 01101010 11100011

Algorithm: Data_Steganography()
INPUT: Carrier image,Noise-like share.
OUTPUT: Stego-image.

1.Load any natural image as carrier image.
2.Load the noise-like share.
3.Calculte the space available for hiding the data.
4.for each pixel in carrier image repeat steps 5-6
5.hide the data in the 2 LSB's of pixel.
6.Reconstruct the pixel using offset.
7.End of the LOOP.
8.Hide the random data 0 or 1 in the remaining pixels
9.Output
10.End.

D.Watermarking-

The watermarking is applied to meaningful shares. The watermarking technique involves use of α-channel of the respective pixel.The shares are transmitted over an unsecured network. This method is for checking of any interception by third party to the shares.

ALGORITHM: Digital_Watermarking()
INPUT: N1,N2,N3 natural share.
OUTPUT: N1,N2,N3 Tga image.

1.Load a natural image.
2.for each pixel in an image repeat steps 3-4
3.Calculate the pixel black or white.
4.Store the respective value in α-channel of the pixel.
5.Reconstruct the value at receiver side.
6.If verified to be true;
7.Output & end else
8.Abort the further process.
9.End.

E.Decryption-

The encrypted image is decrypted using the same key generated from the meaningful shares. To retrieve the original image it is necessary to generate the same key sequence.

ALGORITHM: Decryption ( )
INPUT: S_SHARE
OUTPUT: secret image

1. Stego Image is read
2. LSB bit is calculated
3. Noisy share is extracted
4. The Meaningful image is accessed from the appropriate websites or disk drives.

5. Generate the chaotic equation from the natural images
6. Swap the pixels of the noisy share
7. End

IV.CONCLUSION

The proposed system can share a digital image using diverse image media. The media that include *n*-1 randomly chosen images which are secured using watermarking. The noise-like share is generated based on these natural shares and the secret image in the encryption phase. The steganography is applied to the secret image to provide the higher security. The shares are distributed among the collaborating parties. The retrieval of original image is possible only if all the n-shares remain uninterrupted. The key generated from the n-shares play an important role in the security of the system. The digital shares can be stored in a participant's digital devices. The proposed system provides three level security which proves difficult to break. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants.

REFERENCES

[1] Kai-Hui Lee,Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media" IEEE transactions on Information Forensics and Security , vol 9 no 1 ,January 2014 , pp 88-98.

[2] Moni Naor,Adi Shamir "Visual Cryptography"Eurocrypt ,1994,pp1-11.

[3] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol 7 no1, Feb. 2012,pp. 219–229,.

[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] Inkoo Kang,Gonzalo R.Arce,Heung-Kyu Lee "Color Extended Visual Cryptography using error diffusion" , *IEEE Trans. Image Process.*, vol. 20, no. 1, , Jan. 2011,pp. 132–145.

[6] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image Sharing scheme with reversible steganography based on cellular automata,"*J. Syst. Softw.*, vol. 85, no. 8 , Aug. 2012 pp 1852–1863.

[7] Sadan Ekdemir,XunXunWo , *Digital Halftoning,Project in mputational Science Report,* January 2011,pp1 34.

[8] Natapon Pantuwong , Nopporn Chotikakamthorn,"Alpha Channel Digital Image Watermarking Method", IEEE ICSP Proceedings,2008,pp 880-883.

[9] Pradosh Bandyopadhyay,Soumik Das,Atal Chaudhuri,Monalisa Banerjee,"A new Invisible Color Image Watermarking Framework through Alpha Channel",March 30 2012,pp. 302-308.

[10] Zhongmin Wang,Gonzalo R.Arce,Giovanni Di Crescenzo, "Halftone Visual Cryptography via error diffusion", *IEEE Trans. Inf. Forensics Security,vol 4no 3,September 2009,pp.383-396.*

[11] Weiqi Luo , Fangjun Huang , Jiwu Huang , *Edge Adaptive Image Steganography Based on LSB Matching Revisited,IEEE Trans Inf. Forensics Security,* vol 5no 2,June 2010,pp 201 214.

[12] A. Nissar and A. H. Mir, *Classification of steganalysis techniques: A study , Digital. Signal Process"',* vol. 20, no. 6, Dec. 2010,pp. 17581770.

[13] P.L.Chiu K.H.Lee,K.W.Peng and S.Y. Cheng,"A new color image sharing scheme with natural shadows,"in Proc.10th WCICA ,Being,China,Jul .2012,pp 4-15.