Digital Image Sharing using Encryption Processes

Taniya Rohmetra [1], KshitijAnil Naik [2] , Sayali Saste [3] , Tejan Irla [4]

Graduation Student, Department of Computer Engineering, AISSMS-IOIT, Pune University[1]

Graduation Student, Department of Computer Engineering, AISSMS-IOIT, Pune University[2]

Graduation Student, Department of Computer Engineering, AISSMS-IOIT, Pune University[3]

Graduation Student, Department of Computer Engineering, AISSMS-IOIT, Pune University[4]

ABSTRACT: Secret images can be hidden through Visual Secret Sharing (VSS) schemes in shares that are printed on transparencies or are encoded and stored in a digital form. As the shares include noise like pixels suspicion can surely arise. This suspicion endangers our transmission. Thus VSS schemes suffer largely from a transmission risk problem for the secret itself and in turn for the participants involved. This problem should be dealt with so our process does not include the transmission of any noisy shares. We propose an excellent approach that includes encrypting the image at various levels and using Steganography to avoid transmission risks. Our Experimental results indicate the same.

KEYWORDS: Visual Secret Sharing Scheme, Natural images, Encryption, Steganography.

I. Introduction

Visual Cryptography is a technique which includes encrypting a secret image with each participant holding one or more shares. One has to have all the shares to reveal the actual content of the original image. The secret images may include a picture, a map or any handwritten documents. Securely sharing these images in computer aided environments has become an important requirement today. Traditional techniques include sharing of images split into a number of noisy share. These noisy shares are bound to attract attackers, on the grounds of suspicion. Moreover as the number of noisy shares increases so does the task of managing these shares. Thus techniques which use noisy shares can be termed unsafe. Our process encloses the noisy shares into a carrier image using steganography. As the noisy shares are concealed, the risk of suspicion through attackers becomes minimalistic. Our approach includes transmission of n number of random meaningful images along with 'THE' secret image. The secret image is encrypted using a number of strong algorithms like Jarvis Halftoning which would be discussed further in detail. The contents of the random images also play a part in the encryption of the secret image. Finally the encrypted secret image which would be noisy is concealed behind a carrier image. Transmission process includes, sending of n+1 images(n random +encrypted secret image concealed inside the carrier image) The receiver can get the original secret image by following the reverse process of decryption.

II. Related work

Existing System:
In the Existing system, the algorithm for visual cryptography scheme has been implemented for splitting of the secret image into n number of shares. During transmission of the n shares through the network, if anyone of the share has been tampered with by an unauthorized user, the receiver cannot recover the secret image. If the image is not tampered with, then after the intended receiver receives all the images, the process of superimposition by merging to get back the image is performed. The image that is transmitted to the receiver is in the form of noisy share. This raises suspicion, hence making it unsafe to transmit. The following fig---- shows the existing system.

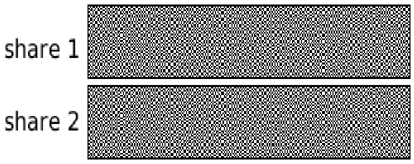


Fig1.0. shows two noisy shares.

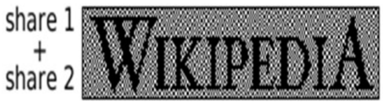


Fig1.1.noisy shares are combined to show the image.

The Proposed System:
In the proposed system, the meaningful shares can be colourful or grey images of family, scenery, hand painted pictures, web images or even personal photographs. The meaningful shares can be in printed form or in digital form. During the encryption process features are extracted from the meaningful shares, it will not make any changes in

the actual image. These features are then hidden behind a carrier image using the process of Steganography. Finally this carrier image is sent to the desired recipient. Now at the receiver end, for performing decryption, the meaningful shares along with the carrier image and decrypted and the original image is reproduced. The flow of the entire proposed system is shown in the fig-----.

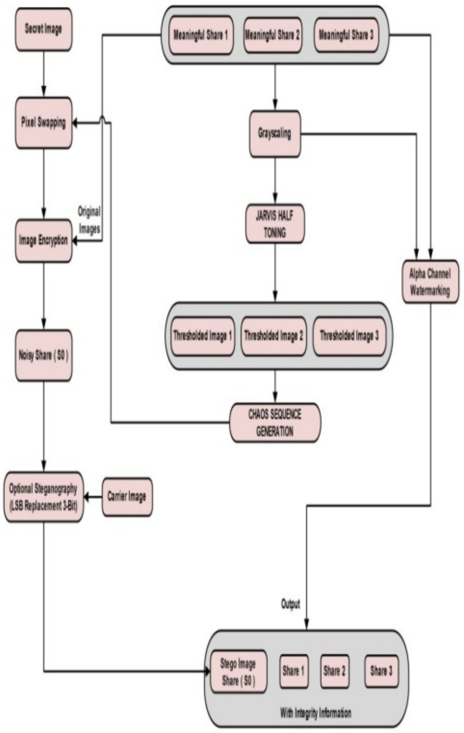


Fig:2.0. Shows the flow of the proposed system.

III. ALGORITHMS

1.Alpha Channel:

In graphics, a portion of each pixel's data that is reserved for transparency information. This transparency information is represented by an alpha channel. The alpha channel is a colour component that represents the degree of transparency. Alpha channel basically adds an additional layer of transparency. An alpha value of zero represents full transparency, and a value of 1 represents a fully opaque pixel. In our system we load the 3 meaningful images and then add an alpha channel to each image. Then during the addition of alpha channel, the 24bit image is transformed into a 32bit image, adding an 8bit transparent layer to the initial image. In our system we are using the alpha channel for verification of the authencity of the images for security purpose that no one tampers with them during the transmission.

2. Jarvis Halftoning:

For the purpose of performing thresholding to the three meaningful images, we make use the Jarvis halftoning algorithm. In the process of thresholding, the pixel of the greyscale image is considered and each pixel is checked wether it is greater than or less than the threshold value (127). If the pixel is greater than 127, it's filled with black otherwise filled with white. The result of this basic method of thresholding is an image with blobs of black and white.

Fig.3.0.shows Lila's images after grey scaling.

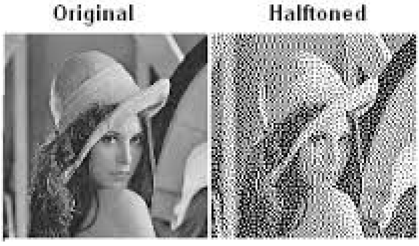


Fig3.1.shows Lilas image after halftoning is performed.

To have a clearer view of the threshold image we use Jarvis thresholding Algorithm. This algorithm makes use of error diffusion method. Error diffusion produces an image of much higher quality than the others. It quantifies each pixel using a neighbourhood operation. The error diffusion scans the image one row at a time and one pixel at a time. The current pixel is compared to a threshold (127) value. If it is above the value a white pixel is generated in the resulting image. If the pixel is below the half way value, a black pixel is generated. The generated pixel is either full bright or full black. Two error diffusion weight matrixes (a) Jarvis, Judice and Ninke (b) Floyd and Steinberg Error are calculated, which is the difference between original image and halftone image. The error is then added to the next pixel in the image and the process repeats. How this error is pushed is decided by an error diffusion matrix.

Error diffusion is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Its main use is to convert a multi-level image into a binary image, though it has other applications. Unlike many other halftoning methods, error diffusion is classified as an area operation, because what the algorithm does at one location influences what happens at other locations. This means buffering is required, and complicates parallel processing. Point operations, such as ordered dither, do not have these complications. Error diffusion has the tendency to enhance edges in an image. This can make text in images more readable than in other halftoning techniques.

3. Chaos Sequence:

Henon map was first introduced by Mivheeal henon. HENON map is a discrete time dynamic system. It is one of the most studied example of dynamic system that exhibit chaotic behaviour.

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n . \end{cases}$$

Fig:3.3.Equation for the henon map.

The map depends on two parameters, a and b which for the classical henon map have values as A=1.4 and B=0.3. Only for these values the henon map is chaotic. Other values may be chaotic or may converge to a periodic orbit. Chaos shuffling will be performed using this henon map technique. Now in chaos shuffling the positions of the pixels of an image will be scrambled in a way depending upon the chaotic map equation. And then again can be regenerated to its original positions by following the decryption process.

Once the meaningful images are added and further processed a random KEY is generated. Using this random key, the A, B values and using the chaos sequence the encryption process will be carried out.

Algorithm for encryption process:

Steps:

1. initialize the for loop with value i=0 with the condition of I as i<=maxlength-1
2. using the following formulae the shuffling will work
3. x1 = 1 + y0 - (a * x0 * x0);
4. y1 = b * x0 The values will then be stored in an array shuffle[i]
5. :check the 2 conditions:
6. if (shuffle[i] < 0) then make the value of shuffle[i] = 0;
7. if (shuffle[i] >= maxLength) then make the value of shuffle[i] = maxLength – 1
8. Updated the values will be stored and the same process will be repeated again.

4. LSB Replacement:

Steganography is a method of hiding digital information so that it will escape detection by unwanted personals. Properly-executed steganography allows for large quantities of information to be hidden inside a file, while making no perceivable changes to that file's contents. Steganography can be applied to many types of data, including audio, video, and images and can hide any kind of digital information. Unlike encryption, which secures the content of a message, steganography hides the message’s existence.

Least Significant Bit Embeddings (LSB) are a general steganographic technique that may be employed to embed data into a variety of digital media, but one of the most studied applications is using LSB embedding to hide one image inside another. Our work focuses on the aspect that we have to use LSB embeddings to hide our Secret Image(Which would be noisy) inside a carrier image so that our complete act is concealed. Our technique works by replacing some of the information in a given pixel with information from the data in the image.

While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colour that the embedding creates. For example, embedding into the least significant bit changes the colour value by one. Embedding into the second bit-plane can change the colour value by 2. If embedding is performed on the least significant two pixels, the result is that a colour in the cover can be any of four colour after embedding. Our process includes two images one secret and one carrier in which we have to hide our secret image. When we attempt to embed our secret image the MSBs of our secret image replace the LSBs of our carrier image, it can be explained in more detail as follows:

a) We know that every pixel has a certain RGB(RED BLUE GREEN) value.
b) The MSBs of 'R' bit of a pixel of the secret image replace the LSBs of 'R' bit of a pixel of the carrier image.
   c) Same happens with Blue(B) and Green(G) bits.
   d) The pixels of the carrier image which would be unaffected, we are going to modify them with replacing the LSBs with some noise thereby increasing security.

IV. Experimental Results

In the experimental setup that we have made, three meaningful images are taken and then the process of encryption is performed on them.

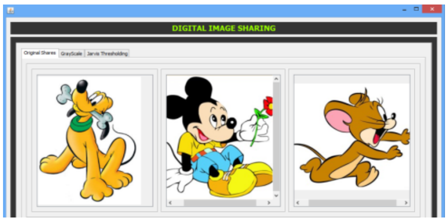


Fig :4.1 this is a screen shot taken which shows three meaningful images loaded.

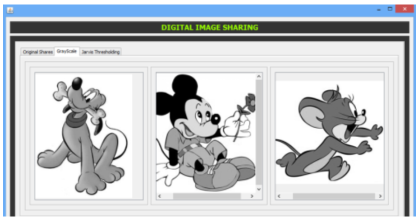
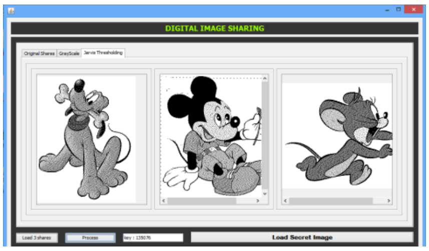


Fig: 4.2 This is a screen shot after the process of Grey scaling is done.

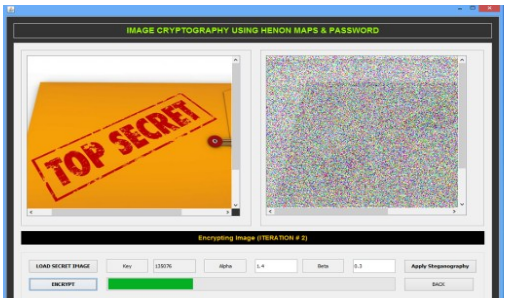
We perform the process of binarization on these three images. The images are grey scaled and thresholded.



key : 135076

Fig :4.3 This screen shot shows the result of Jarvis halftoning.

As seen in the picture above, error diffusion produces an image of much higher quality than the others.
As seen above a key is generated using the number of white and black pixels, this key will be further used for encryption.

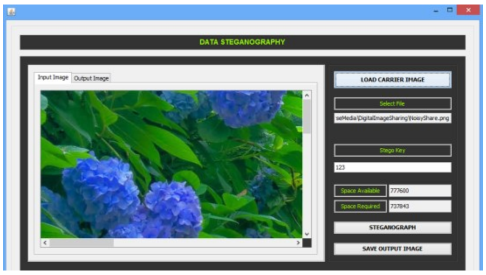


Encrypting Image (ITERATION # 2)

Key 135076
Alpha 1.4
Beta 0.3

Fig: 4.4 This is a screen shot taken of encryption of the secret image.

The secret image is loaded and encrypted with the help of chaos sequence; encryption is performed using the key generated by the three images in the fig. And the secret image, hence creating a noisy share.



Select File: seMedia\DigitalImageSharing\NoisyShare.png

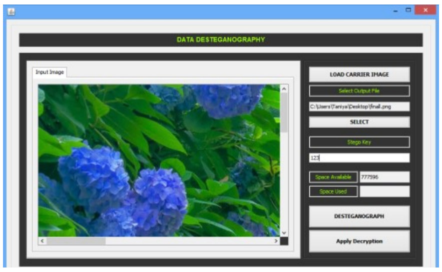
Stego Key: 123

Space Available: 777600

Space Required: 737843

Fig 4.5This is a screen shot taken which shows steganography.

A carrier image is loaded to hide the noisy share. The size of the carrier image is larger than the previous images used. A stego key is put, like a password that will be used during the decryption process.



Select Output File: C:\Users\Taniya\Desktop\final.png

Stego Key: 123

Space Available: 777596

Space Used:

Fig 4.6This is a screen shot taken that shows the desteganography of the encrypted image.

Now at the receivers end, we will perform desteganography using the same stego key that was used previously. The noisy image is separated from the carrier image and will be decrypted further.

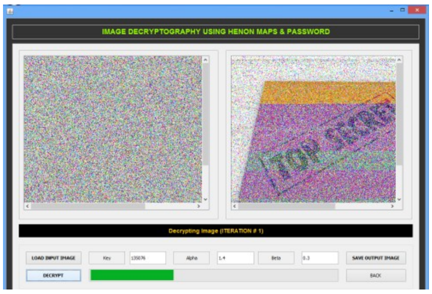


IMAGE DECRYPTOGRAPHY USING HENON MAPS & PASSWORD

Decrypting Image (ITERATION # 1)

Key 135076 Alpha 1.4 Beta 0.3

Fig 4.7This is a screen shot taken that represents the decryption of the secret image.

During the decryption, the key generated during the encryption will be regenerated using the meaningful images and then the process of dencryption will be performed as seen in the figure.

V. Conclusion

We have implemented a project that will overcome the difficulties of VISUAL CRYPTOGRAPHY. Though the current encryption process is very much secure, but still with the help of advancement in the technology we can build a more secure system by adding an additional layer of security to the existing one.

IV. REFERENCE

[1] Steganography algorithm for hiding image in image by improved lsb substitution by minimize detection, Vijay Kumar Sharma ,Vishal Shrivastava

[2] An Approach to Digital Halftone Processing Using Error Diffusion in Forward and Backward Direction. Deepak Sharma, Deepti Sharma Vikas Sindhu MDU, Rohtak Assistant Professor, MDU, Rohtak Haryana, India Haryana, India.

[3] Chaos image encryption using pixel shuffling with henon mapManjunath Prasad and K.L.Sudha Department of ECE, DSCE, Bangalore.

[4] Secret sharing schemes with diverse image media.G. Selvapriya, J. Jayapriya Jayapal

[5] Digital image sharing by diverse image media, Kai-Hui Lee and Pei-Ling Chiu.

[6] 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

Sayali Rajendra Saste is a student pursuing her B.E. Degree under Department Of Computer Engineering from University Of Pune. She has been working actively on the project. She has specially worked over the literature survey, mathematical model and the Alpha Channel Embedding Algorithm.

Taniya Rohmetra is a student pursuing her B.E. Degree under Department Of Computer Engineering from University Of Pune. She has been working actively on the project. She has specially worked over the literature surveys, project planner and Jarvis Halftoning Algorithm.

Kshitij Naik is a student pursuing his B.E. Degree under Department Of Computer Engineering from University Of Pune. He has been working actively on the project. He has specially worked over the literature surveys, mathematical model and the Chaos Shuffling Algorithm.

Tejan Irla is a student pursuing his B.E. Degree under Department Of Computer Engineering from University Of Pune. He has been working actively on the project. He has specially worked over the literature surveys, project planner and the LSB Replacement Algorithm.