Implementation Paper on Visual Cryptography for Sharing Digital Image Using Diverse Media

Aparna Choudhari[1], Sampada Murhe[2], Ashwini Kalekar[3],Assoc.Prof.Trupti Suryawanshi[4].

[1,2,3]BE in Computer Engg.KSE,Pune,Maharashtra,India.
[4]Assoc.Professor in Computer Engg.KSE,Pune,Maharashtra,India.

---***---

Abstract – As we know that today's era is working on very advance techniques with internet and t*raditional encryption techniques are just converting the readable images into some unreadable format i.e. cipher text format. This encrypted cipher text can be very conveniently transmitted over the network, but anyone who gets the key can easily get the secret encrypted message from cipher text, but the new and advance Secret sharing scheme is a process of sharing and transmitting the images over the network. But the major drawback over here is that transmitting images over network pulls attackers attention as the images are in noise like format. In the recent study, many researchers tried to make the VSS system more secure. This paper shows the survey of the studies done earlier and thereby analyses the drawbacks and proposed a new technique considering VSS.*

Key Words: *Visual Secret Sharing Scheme, Natural image, Encryption, Steganography, Cryptography.*

1. INTRODUCTION

The rapid growth of internet and internet services which needs connecting multiple devices , computers together so that the transmission of the data can be carried out needs a higher level of security in this stage. Traditional encryption techniques are just converting the readable images into some unreadable format i.e. cipher text format. Encryption process is the process of using the hash function and indirectly a mathematical function that makes the data get converted into unreadable format which is safe for transmitting over the internet.

Using the conventional Image sharing, which can contain several random and useless pixels, even if these image sharing techniques satisfy the security requirement for safeguarding the secret data, but it is prone to some issues such as attackers attention as the images are noise like, and second issue is that these noise like meaningless shares are very user unfriendly. If the count of the shares being shared and the share quality is enhanced, then it can become trickier and difficult to expose the necessary information.

The process in which n pieces of images or shares carry each share into it is called as Visual Cryptograph (VC). Secret images can be in the form of handwritten documents, images, photographs and so on. Sharing and delivering secret images over the internet in the non-computer environment is a process of Visual Secret Sharing.

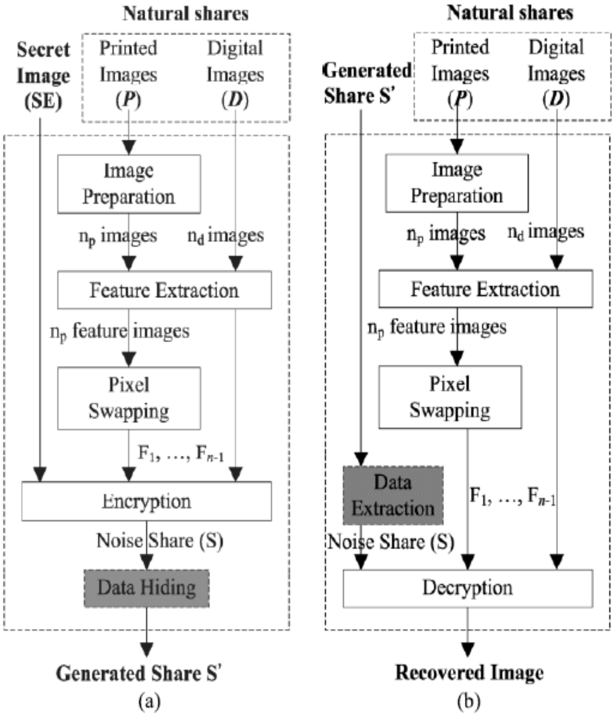


Figure 1. System working of [1] system

2. Literature Survey

A. A simulated annealing algorithm for general threshold visual cryptography scheme

P. L. Chiu and K. H. Lee proposed a pixel-expansion-free value VCSs method on the basis of optimal binarization technique for visual cryptography of binary images. To grade the evaluation of the quality of the extracted or recovered image, author considered the black pixels or blackness as the metric to measure quality.

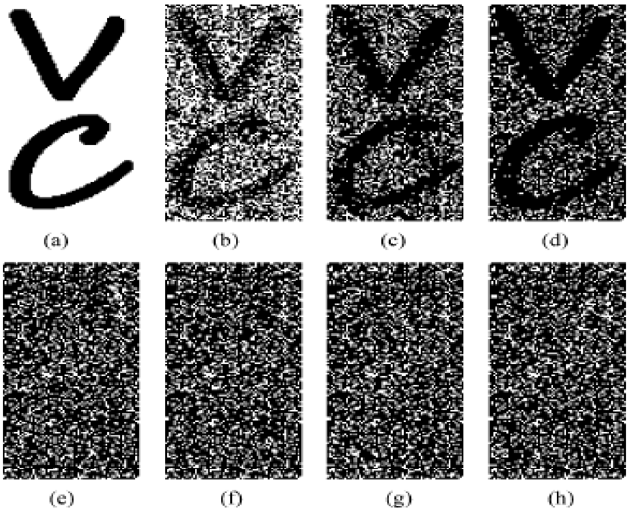


Figure 2. Image stages in [2] system

Their contribution is proposed as a two-fold method, first fold is formulating the problem as an optimization using mathematics and in return to highly increase the contrast of extracted images that are lead to blackness constraints and density-balance, and second they proposed a new AI based simulated-annealing algorithm to solve this VSS problem. The proposed optimization-based approach efficiently competes existing techniques in terms of both the display quality of recovered images and pixel expansion factor [2].

B. Image size invariant visual cryptography for general access structures subject to display quality constraints

K. H. Lee and P. L. Chiu presented visual cryptography faces an uncontrollable display quality issues or a pixel-expansion problem, for extracted images. To resolve these issues in paper, author proposed a systematic and general method without convenient codebook design. This presented technique can be definitely used for binary secret images in non-computer controlled decryption environments. So To encrypt secret data pixels author proposes a set of column vectors method rather than using the traditional VC-based method to address issue of pixel expansion [3].

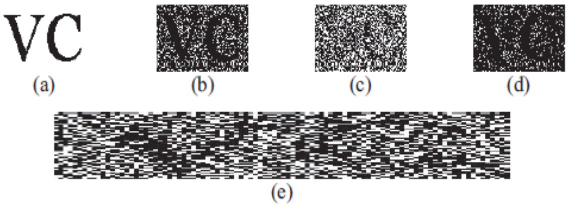


Fig. 4. Comparison between other approaches and the proposed study on the worst case result (i.e., set {1, 2, 3}) of access structure {{1, 2, 3}, {1, 4}, {3, 4}}, (a) Secret image with 96 × 64 pixels (192 DPI), (b) the recovered images of this study (contrast $\alpha_{\min} = 2/9$, blackness $\beta = 1$), (c) the recovered image of Hsu's study ($\alpha_{\min} = 0.15$, $\beta = 0.75$), (d) the recovered image of Lee's study ($\alpha_{\min} = 1/8$, $\beta = 1$), (e) the recovered image of Ateniese's study (pixel expansion factor = 5, $\alpha_{\min} = 1/5$, $\beta = 0.8$).

Figure 3. Comparison with existing and system [3]

C. Halftone visual cryptography via error diffusion

Z. Wang, G. R. Arce, and G. D. Crescenzo presented a novel framework named as halftone visual cryptography to obtain visual cryptography through half toning based on blue noise dithering technique, the presented method makes use of the void and cluster algorithm to encrypt a secret binary image into halftone shares carrying significant visual information. The obtained visual quality is much better than all previous visual cryptography techniques. The proposed technique has multiple visual secret sharing applications such as watermarking, electronic cash which requires a very high-quality visual images [4].

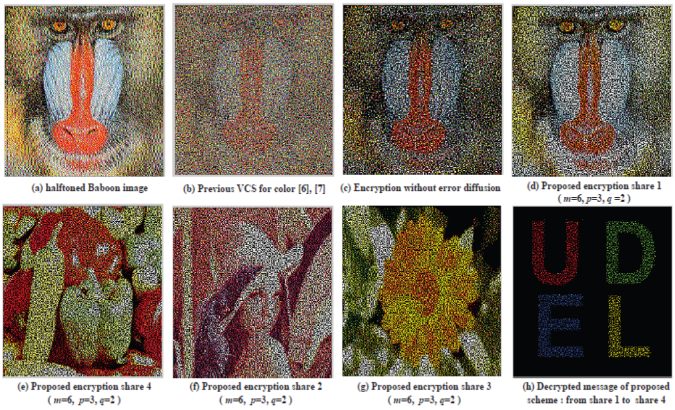

(a) halftoned Baboon image
(b) Previous VCS for color [6], [7]
(c) Encryption without error diffusion
(d) Proposed encryption share 1 (m=6, p=3, q =2)
(e) Proposed encryption share 4 (m=6, p=3, q=2)
(f) Proposed encryption share 2 (m=6, p=3, q=2)
(g) Proposed encryption share 3 (m=6, p=3, q=2)
(h) Decrypted message of proposed scheme : from share 1 to share 4

Figure 4. Comparison of existing system with system [4]

D. Color extended visual cryptography using error diffusion

I. Kang, G. R. Arce, and H. K. Lee presented phenomenon known as a color visual cryptography process which prepares meaningful color n shares via error diffusion and Visual information pixel synchronization for visual sharing recovered quality improvement. Visual information pixel synchronization preserves the same original VIP values pre and post encryption and error diffusion then generates n shares with higher` visual quality. VIP synchronization or error diffusion mostly used in various visual cryptography schemes for color images. As compare with previous approaches proposed approach gives superior performance [5].

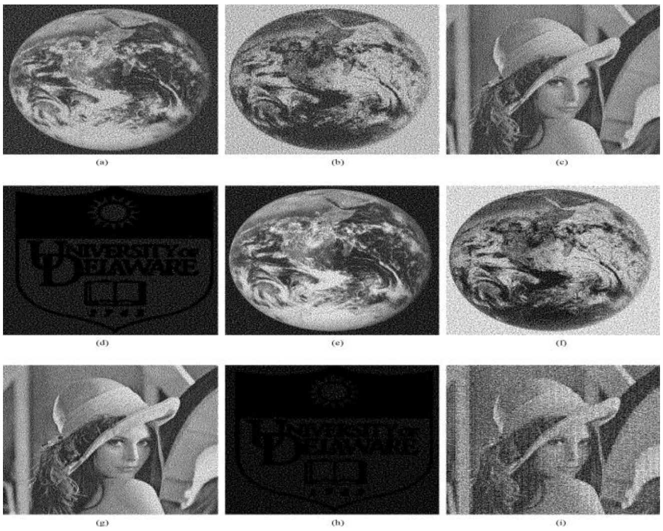


Figure 5. Comparison of existing systems with system [5]

E. A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images

T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le presented a new secret sharing scheme for grayscale images. Proposed scheme is based on three approaches, block truncation coding (BTC), discrete wavelet transform (DWT) and vector quantization (VQ) technique. An original image is replaced with a set of much smaller shadows and each shadow does not reveal information about the original image. Due to this quality the security of the proposed scheme is guaranteed. This proposed scheme can be applied to both grayscale and color images. Results confirm that this scheme not only generates a high quality reconstructed original image but also generates small, random-like grayscale shadows [6].

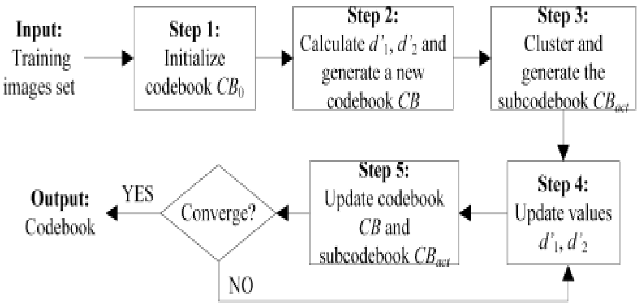

Input: Training images set
Step 1: Initialize codebook CB_0
Step 2: Calculate d'_1, d'_2 and generate a new codebook CB
Step 3: Cluster and generate the subcodebook CB_{act}
Step 4: Update values d'_1, d'_2
Step 5: Update codebook CB and subcodebook CB_{act}
Converge?
YES
NO
Output: Codebook

Figure 6. Codebooks generation algorithm [6]

F. A novel secret image sharing scheme for true-color images with size constraint

D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang proposed a novel and efficient secret image sharing scheme for true-color secret images. By combing neural networks and variant visual secret sharing, the quality of the reconstructed secret image and disguise images are visually the same as the original images. Only proposed scheme supports true-color secret image with size constraint on shares as compare to other[7].

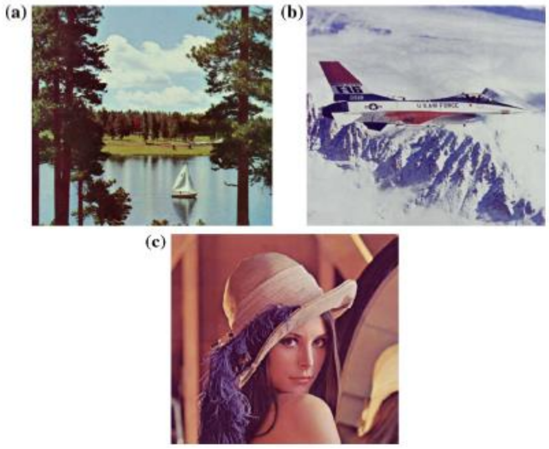


Figure 7. Camouflage images: (a) Boat, (b) F16 (size of both nine times that of the secret image). Reconstructed secret image (c) Lena.

D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang proposed anew secret image sharing scheme with reversible steganography. A reversible cellular automaton with memory is added in the proposed scheme to produce shared data, which are implanted into cover image to form stego images. Computation cost of the proposed scheme is lower than other approaches. The proposed scheme is useless in differential attacks[8].

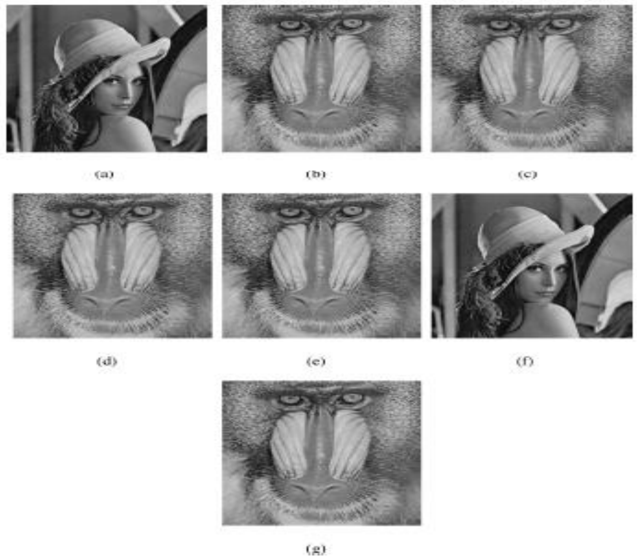


Figure 8. An example of the (4,4)-threshold case with reversible steganography. (a) The secret image, (b) stego image S1, PSNR = 37.91 dB, (c) stego image S2, PSNR = 37.90 dB, (d) stego image S3, PSNR = 37.91 dB, (e) stego image S4, PSNR = 37.92 dB, (f) lossless reconstruction of the secret image, and (g) the distortion-free recovered cover image.

3. Proposed System

The proposed system in itself in a single entity but to achieve the aim from the project, it needs to be divided into following proposed modules.

Sender Module

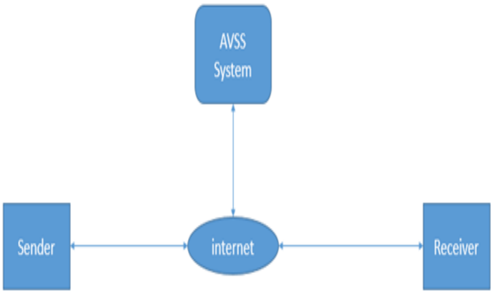
Sender Module takes care of the below operations:

- Splitting the secret image to be transmitted into n pieces (n will be a threshold being decided after later system analysis).: The secret image is a matrix of pixels and hence has two dimensions, so the image can be split into small pieces of images by considering small portion of image pixels at a time. Thus image is split into n pieces by computing the size as follows: assumption, the image is split into 4x4 i.e. n=16 matrix of small images. So the formula to decide the size of the splitted images will be: If h is image height and w is image width: Height of single image piece=h/4 and width of single image piece = w/4;

- Shuffling the pieces randomly so as to make the visual data non understandable and thereby deforming the original data. As the splitted images are numbered as per the sequence, so to shuffle the images, just the numbers are needed to be shuffled and the random numbers obtained after shuffling are the sequence of embedding the n pieces in the n natural images.

- Embedding each ‘n’ shuffled piece of secret image into ‘n’ natural images used as cover image for transmitting the secret image. To embed the image into natural image, LSB steganography technique is used. LSB substitution technique is the most efficient technique for embedding the images or data into another image.

- Encrypting the shuffled sequence of the ‘n’ pieces of the secret image and sending the same to the receiver’s mail id. The encryption process is a novel encryption technique which first coverts the data to be encrypted into corresponding ASCII values, then the key i.e. any 3 digit whole number without any zero digit, and add the numbers into ascii values in a specified sequence of normal digits squared digits and cube digits and repeating the pattern till the data length is matched.



Receiver Module

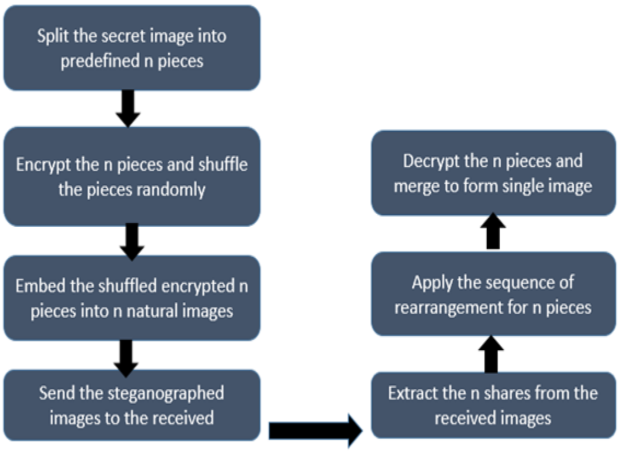
- At receiver end retrieving the embedded ‘n’ pieces of secret image from n received natural images.

- Decrypting the received sequence over mail and providing the retrieved sequence to the system for rearranging the retrieved pieces of images.

- Merging the rearranged 'n' pieces of the secret image.

Notification Module

The notification module is responsible to send the sequence of rearrangement and decryption key for receiver to get the secret data.


Split the secret image into predefined n pieces
Encrypt the n pieces and shuffle the pieces randomly
Embed the shuffled encrypted n pieces into n natural images
Send the steganographed images to the received
Extract the n shares from the received images
Apply the sequence of rearrangement for n pieces
Decrypt the n pieces and merge to form single image

4. Mathematical Model

The proposed system can be mathematically represented as following sets and corresponding set operations:
Set S = {s1, s2, s3, s4, s5, s6}
Where,
s1= Selecting secret image to be sent.
s2= splitting the secret image into n pieces.
s3 = encrypting the splitted image pieces.
s4 = shuffling the n pieces.
s5 = embedding the n pieces into n natural images.
s6= sending the n natural images to receiver.

Set R = {r1, r2, r3, r4, s6, c3}
Where,
r1= Extracting the n pieces from the n natural images.
r2= decrypting the n extracted pieces.
r3 = rearranging the pieces as per received sequence.
r4 = merging the n pieces to form 1 image.

Set C = {c1, c2, c3, s6, s4}
Where,
c1= Get shuffled sequence of n pieces.
c2= get decryption key of n images.
c3 = send the notification mail to receiver.

δ: Q [∑ q0] →q1
Here, the system transits form initial state to state q1.
Where, q1 selecting secret image to be sent and splitting into n pieces.

δ: Q [∑ q1] → q2
Here, the system transits form q1 to state q2.
Where, q2 is encrypting the n pieces before embedding into natural images.

δ: Q [∑ q2] → q3
Here, the system transits form q2 state to state q3.
Where, q3 is shuffling the splitted pieces randomly.

δ: Q [∑ q3] → q4
Here, the system transits form q3 state to state q4.
Where, q4is embedding the encrypted images into n natural images.

δ: Q [∑ q4] → q5
Here, the system transits form q4 state to state q5.
Where, q5 Notifying the receiver through mail regarding sequence of pieces and decryption key.

δ: Q [∑ q5] → q6
Here, the system transits form q5 state to state q6.
Where, q6 is sending the stego images to the receiver.

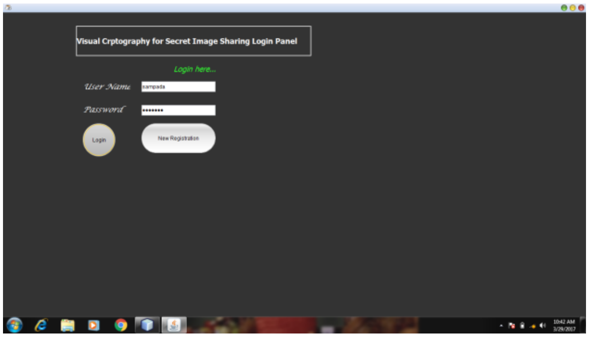
δ: Q [∑ q6] → q7
Here, the system transits form q6 state to state q7.
Where, q7 is receiver extracting the n pieces from natural images.

δ: Q [∑ q7] → q8
Here, the system transits form q7 state to state q8.
Where, q8 decrypting the extracted n pieces of image.
δ: Q [∑ q8] → q9
Here, the system transits form q8 state to state q9.
Where, q9 is rearranging the n pieces as per received notification of piece sequence.

5. Results

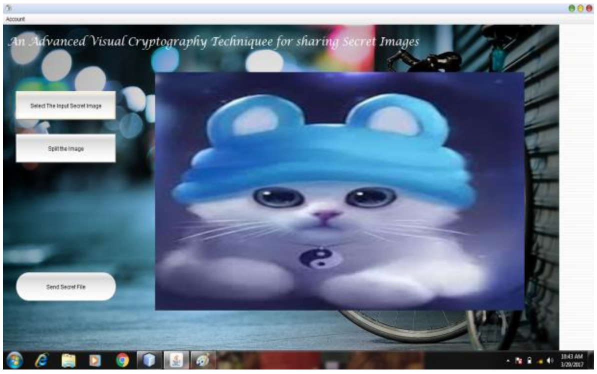
Proposed system results are as shown below:

Login Page

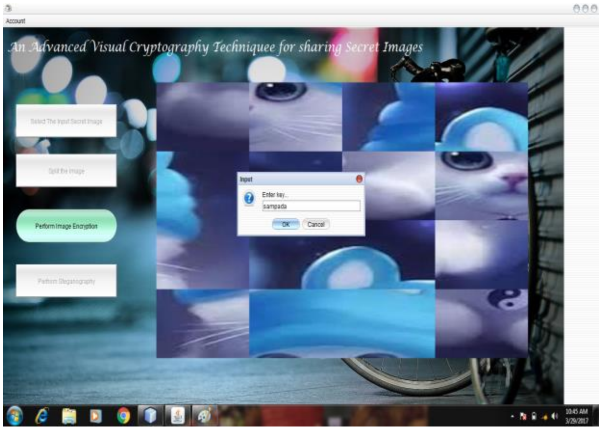


User Name: sampada
Password: •••••••

Selection of Secret Image

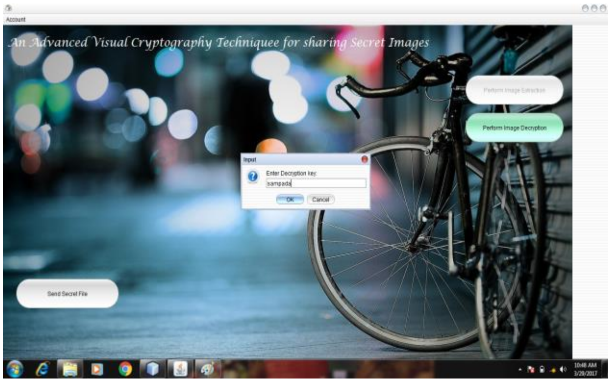

Account
An Advanced Visual Cryptography Techniquee for sharing Secret Images
Select The Input Secret Image
Split the Image
Send Secret File

Split the input image with encryption key


Account
An Advanced Visual Cryptography Techniquee for sharing Secret Images
Select The Input Secret Image
Split the Image
Perform Image Encryption
Perform Steganography
Input
OK
Cancel

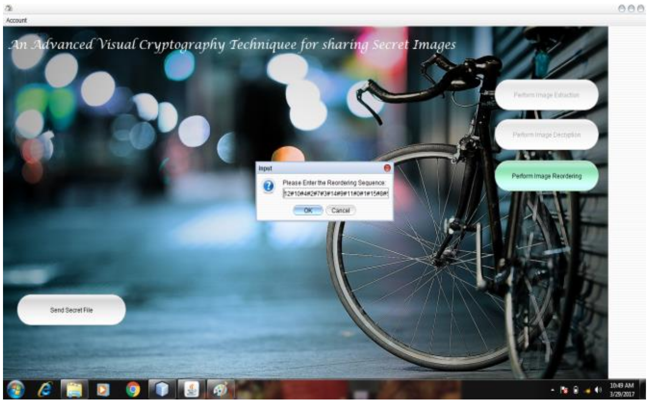
Enter key...
sampada

Decrypt the image with encryption key



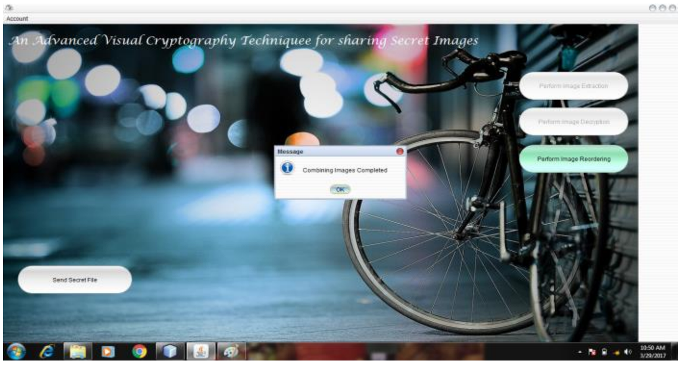
Enter Decryption key:
sampada

Reordering the splitted image after decryption operation



Please Enter the Reordering Sequence:
12#10#4#2#7#3#14#9#11#0#1#15#8#

Image reordering succeesfull



Combining Images Completed

Conclusion

Thus this paper presented an all-inclusive survey of secret sharing scheme. The main features, the advantages and disadvantages of each are described. As per survey, strong need to develop the secure secrete scheme for sharing images over network. In proposed work is the combination of data hiding, random shuffling and the encryption technique. Using this we achieve the original image with security.

REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu,"Digital Image Sharing by Diverse Image Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images," Digit. Signal Process., vol. 21, no. 6, pp. 734–745, Dec. 2011.

[7] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secret image sharing scheme for true-color images with size constraint," Inf. Sci., vol. 179, no. 19, pp. 3247–3254, Sep. 2009.

[8] 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, pp. 1852–1863, Aug. 2012.

BIOGRAPHIES

I, Aparna Choudhari, am a final year student of Computer Engg Dept. in Keystone School of Engg Deemed University college of Engineering Pune.

I, Sampada Murhe, am a final year student of Computer Engg Dept. in

I, Ashwini Kalekar, am a final year student of Computer Engg Dept. in Keystone School of Engg Deemed University college of Engineering Pune

I, Trupti Surywanshi, am an Associate Professor in Computer Engg Dept. in Keystone School of Engg Deemed University college of Engineering Pune.