ISSN : 2494-9150 Vol-02, Issue 01, APR 2016.

Visual Cryptography with Watermarking over Color Image

[1]Varsha Hole (Guide), [2]Apurva Naik, [3]Roshni Patil, [4]Ankit Tiwari
[1,2,3,4]Computer Engineering Dept, Smt. Indira Gandhi College of Engineering, Mumbai, Maharashtra, India
[1]varshahole@gmail.com , [2]apurvasnaik123@gmail.com , [3]roshnia.patil@gmail.com,
[4]tiwariankit2026@gmail.com

Abstract - Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, images, diagrams, maps) to be transmitted in a secured way. The color secret image is split up into shares and watermarked with cover image. It is then transmitted to sender. At the receiving side original image can retrieved if all shares are present. The cover images are extracted from the shares and stacked one by one which reveals the secret image progressively. This scheme provides a more efficient way to hide images in different meaningful shares providing high security and recovered image with high contrast.

Keywords — Visual cryptography, watermarking, shares.

I. INTRODUCTION

The world today relies on the internet for information storage, transmission and retrieval, hence a huge amount of multimedia information is transmitted over the internet. There are some applications where it is required to send various credential data such as military maps, signatures, thumb impressions, confidential model, diagram of project over the internet. While sending these secret images over network security issues should be taken into consideration. Hackers may utilize weak link over communication network to steal information or masquerade it to get the information they want. To deal with security problems of secret images, various image secret sharing schemes have been developed.

Visual Cryptography is one of the latest technique for secret image sharing and used to protect against unauthorized data access and secure dissemination of sensitive information. Visual Cryptography is the technique that encrypts a secret document or Image by breaking it into shares. The secret image can be reconstructed by stacking the shares together, with no complex cryptographic calculations. In this way visual cryptography allows secure transmission of secret images.

Visual cryptography can be used in military applications for sending secret maps, in companies for sending confidential model, diagram of project, in banking field for sending signatures, passwords, thumb impressions etc.

II. LITERATURE SURVEY

To provide security to credential images that are send over the untrusted network various techniques are there which we have surveyed and that techniques we are discussing below.

In Steganography technique, we transfer the entire image by hiding it behind another image, audio, video etc. We hide data into a common object, but if someone extracts it, he/she can get all the information easily. This technique has drawback that if the attacker finds by any means the way to capture the secret image, the entire information can be gained by the attacker, as the data is raw one. Therefore there is a need of some other rigid technique for providing security to the credential images.

A. Basic (2, 2) VC scheme

Visual Cryptography (VC) was first introduced by Noar and Shamir at Eurocrypt'94 [1]. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is Xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Table 1 illustrates the scheme of encoding one pixel in a (2, 2) VC scheme. A white pixel is shared into two identical blocks of sub¬ pixels. A black pixel is shared into two complementary blocks of sub-pixels. While creating the shares, if the given pixel p in the original image is white, then the encoder randomly chooses one of the first two columns of Table 1. If the given pixel p is black, then the

encoder randomly chooses one of the last two columns of Table 1. Each block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. Thus no information is gained by looking at any group of pixels on a share, either.

Pixel	White		Black	
Prob.	50 %	50%	50%	50%
Share 1				
Share 2				
Stack Share 1 & 2				

Table1. Visual Cryptography Scheme

B. VC using unexpanded shares:

Yong-Chang Hou and Zen-Yu Quan [2] design two n × n matrices denoted by C0 and C1 (Table II), which represents the sharing matrix for white and black pixels of the secret image, respectively. Each row in matrix C0 or C1 represents a sharing method, and each column represents the value assigned to every participant (0 is for white, 1 is for black). In matrix C0, the first row is assigned to 1, and other rows are all 0. On the contrary, matrix C1 is a diagonal matrix, which means 1 is assigned to the diagonal line and the rest elements are all 0. Therefore, each pixel on the shares will have only 1/n chance to occur as black disregarding it is dispatched from white or black pixels of the secret image. When sharing a black pixel of the secret image, the black will show at different positions on different shares, which means after stacking more shares the chance of being black for black area of the secret image will be increased. However, when sharing a white pixel of the secret image the position of occurring black on every share is the same; therefore, black will still appear at the same position on the stacked image and the chance of being black for white area of the secret image will remain as 1/n. This will gradually sharpen the black-and- white contrast on the stacked image as more shares are stacked, the hidden content will be progressively revealed. During the dispatching process, random numbers ranging from 1 to n are needed to create shares. To share a white pixel of the input image, we choose a random number l, and distribute the values of the lth row vector of C0 to every share, which means that the first value of row vector [C0 (l, 1)] is distributed to Share1, and the second value [C0 (l, 2)] is distributed to Share2, and so on. By the same token, C1 is applied to share a black pixel with the same sharing steps as sharing a white pixel. The primary issue of a VSS scheme is to safeguard the security. Any column in C0 or C1 only has single "1," that means regardless the color of the pixels of the secret image is white or black, the probability for them to appear 1 on each share is the same as to 1/n, which, therefore, gives no clue to the content of the secret image on the shares.

$$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n} \qquad C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$$

Fig.1 Two m*n secret sharing matrix

Algorithm for Generating Shares Using Unexpanded Share Method

Input: A W × H halftone secret image P where
p (i, j) P

Output: n shares Sm, m=1, 2……., and n
Process:
1). Generate sharing matrices C0 and C1
2). for each pixel p (i, j), 1 <= i<= W, 1<= j<=H
2.1). randomly choose a value l, range from 1 to n
2.2). For m=1, 2,…., and n
2.2.1) If the pixel p (i, j) = 0 (white), the pixel value Sm (i,j) = C0 (l,m)
2.2.2) If the pixel p (i, j) = 1 (black), the pixel value Sm (i,j) = C1(l,m).

C. Watermarking:

The random meaningless shares are hided with cover image to form meaningless shares by using watermarking technique.

Encryption phase of PVC with watermarking:
The secret image is first partitioned into n shares using progressive visual cryptography. Each share is then superimposed with a cover image to generate the meaningful shares, which is then transmitted.

ISSN : 2494-9150 Vol-02, Issue 01, APR 2016.

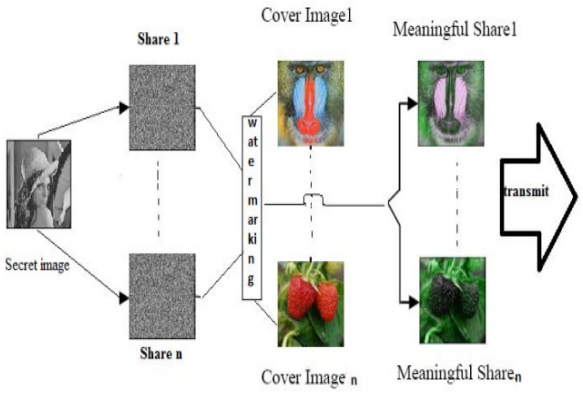


Fig.2 Encryption phase of PVC using watermarking.

Decryption phase of PVC:

In the decryption phase, the original shares are extracted from meaningful shares. This shares are then stacked together to reconstruct original image.

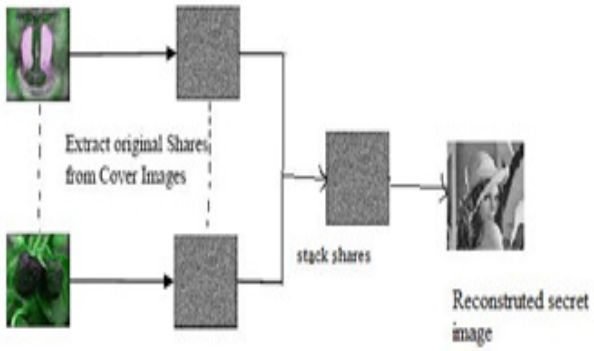


Fig.3 decryption phase of PVC

III. PROPOSED METHOD

Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, images, diagrams, maps) to be transmitted in a secured way. Based on the survey, there are Visual Cryptography techniques proposed which mainly focus on black and white image, further there is encryption and decryption these two phases are included. So to provide more security, we propose a Visual cryptographic method which also work for color images and along with encryption, decryption techniques, a watermarking technique is also added to make it more secure. The color secret image is split up into shares and watermarked with cover image. It is then transmitted to sender. At the receiving side original image can retrieved if all shares are present. The cover images are extracted from the shares and stacked one by one which reveals the secret image progressively.

A. Encryption

User give the secret image to the system and also give patch size and number of slides as a input. The cover image is given.

B. Decryption

During decryption all the watermarked slides, which were created during encryption, will be the input to the decryption software whereas cover image will be the decryption key. The decryption process starts by giving all the watermarked image slides along with the cover image as input to the decryption software. Each watermarked image slide XORed with the cover image and the resultant image will be saved in another blank image slide which is nothing but the single slice of secret image. Thus with each iteration all the slices are generated and simultaneously ORed with the previously generated slices thus forming the original secret image.

IV. IMPLEMENTATION DETAILS

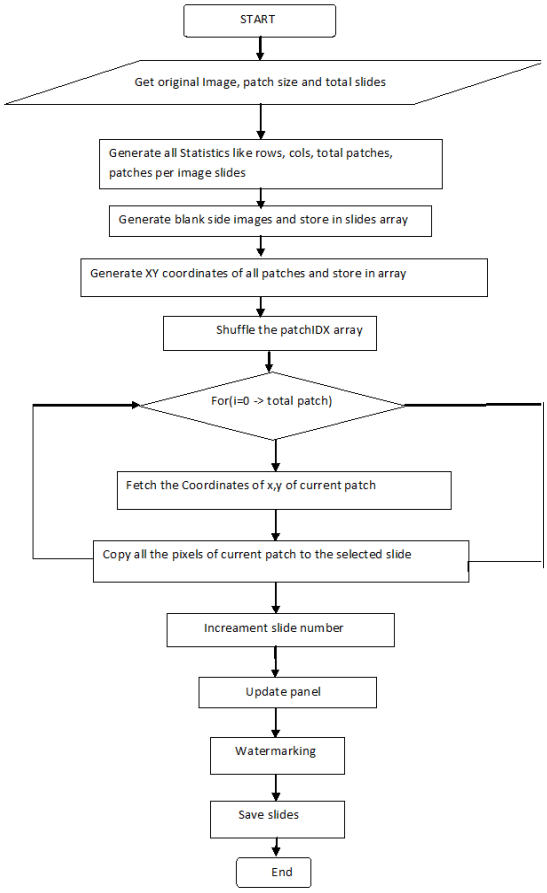
A. Encryption

Algorithm for slicing the original image:
Input: Original image
Output: Meaningful shares of original images
1. Get original image
2. Get patch size and get total slides
3. Generate all statistics like,
   Cols = width / patch size
   Rows = height / patch size
   Total patches = rows * cols
   Patches per slide = total patches / slides
4. Generate blank slide images and store in slide array
5. Generate XY coordinates of all patches and store in patchXY array
6. Generates patchIDX array for shuffling
7. Shuffle the array
8. For(i=0; i<=total patches; i++)
   8.1. Fetch the coordinate of x,y of current patch
   8.2. Copy all the pixels of current patch to the selected slide
9. Increment slide and go to step 8.
10. Update panel
11. Watermarking on shares
12. Save meaningful slides

B. Decryption

Algorithm for stacking the slide images:
Input: All meaningful shares of original images
Output: final image same as original image
1. Open all side images
2. Remove watermarking
3. For (i=o; i<total slides; i++)
   3.1. XOR the all the pixel of current slide and
   3.2. stacked slide
4. Update panel
Save image

C. Flowchart



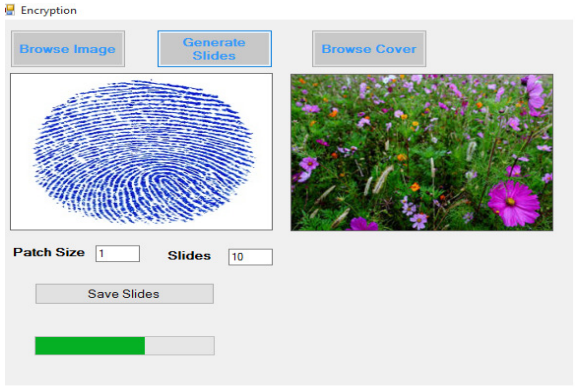


Fig.6 Generate Slides

Fig.7 Stacking Window

D. Screenshots

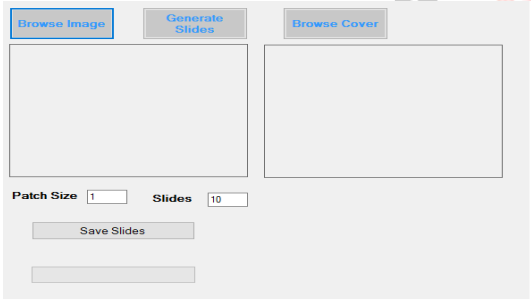


Fig. 4 Slicing Window

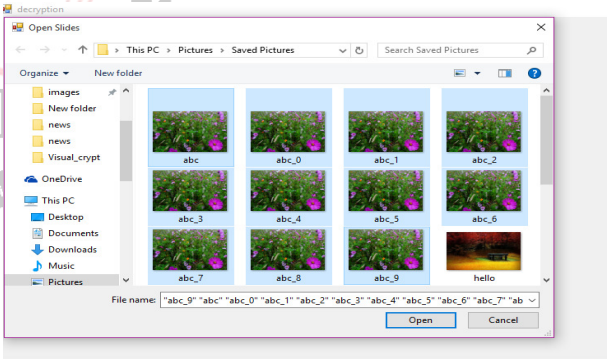


Fig.8 Open Slides

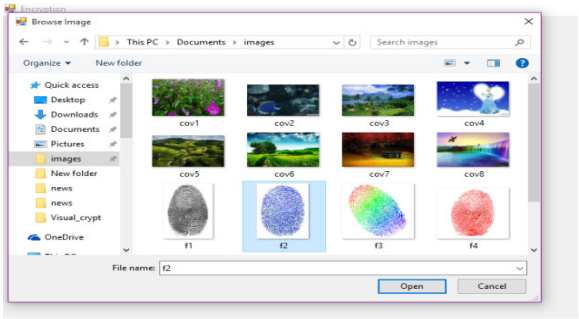


Fig.5. Open secret image

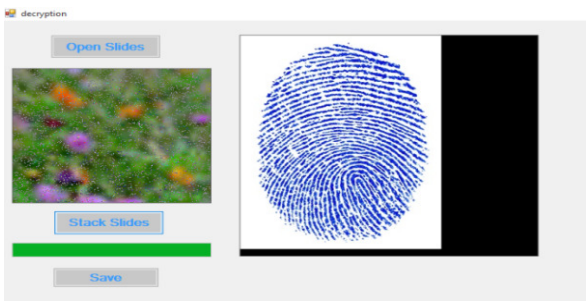


Fig.9 Stacking Window

V. RESULT AND ANALYSIS

The parameters- columns, rows, total number of patches depends on patch size, image height and width. The Patches per slide depend on the number of slides what the user give input to system We are giving the default value 1 for patch size and 10 for slide and we calculate the number of columns, rows, total number of patches using following statistics.

Row=Image Height/Block size
Column=Image width/Block size
Patches=Rows*Column
Total patches per slide=Patches/Total slide

If we increase the patch size then number of rows, columns and total number of patches decreases and security will be reduced. The number of patches per slide depends on the input of number of patches that the user has given to system. If the number of slides is increased then the number of patches per slide decrease and hence there is more security. If both the number of slides and patch size is increased, then number of rows, columns, total patches, patches per slide decreases. If the patch size is less then there is possibility of image being more secure. Our method is more secure as the cover image is the key for decryption which we had used in encryption. If user does not have all the slides, then user will not get the complete information. If user has cover image and 1 or more than 1 slide, then user can get rough idea about the image but whole information will not be revealed. If we take different cover image as decryption key, then user will not get any information.

Patch size	Slides	Columns	Rows	Total patches	Patches/ Slide
1	10	250	345	86250	8625
1	20	250	345	86250	4312
5	10	50	69	3450	345
5	20	50	69	3450	172
1	100	250	345	86520	862

Table2. Testing

VI. CONCLUSION

To provide security to credential images in various fields is important in these days. So we have used Visual Cryptography for that purpose. To make this technique more rigid and user friendly we work on n number of shares and color images. Further to make it more protective we cover meaningless shares using watermarking technique to convert into meaningful shares. In visual cryptography technique original image is divided into multiple meaningful shares for that we are applying watermarking concept and original image can be recovered by stacking all the shares. The quality of the stacked image is same as original image.Overall Performance assessed on four areas: type of share generated, image format, Patch generation, and number of meaningful shares. The project deals with secret image sharing. This is done by dividing a single secret image into multiple numbers of shares. Giving input as a secret image to the system, it generates number of shares according to the user. The multiple shares that are generated can now be sent to the destination. Only when the user on destination side has all the required shares with him of the secret image, the original secret image can be retrieved otherwise the image cannot be retrieved. The system is user friendly and easy to operate.

Thus the project provides security of data in form of image and it has wide applications like in Banking for sharing passwords, Signature, finger prints etc, in Military applications for sending secret maps, images, in Companies for sending confidential model, diagram of project etc.

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography,” in Proc. Adv. Cryptol.: EUROCRYPT, vol. 950. 1995, pp. 1–12.

[2]“Multi-pixel Visual Cryptography for color images with Meaningful Shares” by Ms. KiranKumari et. al. / International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2398-2407.

[3] “Maintaining the Secrecy in Visual Cryptography Schemes”, by Divya.A and K. Ramalakshmi, 978-1-4244 -8679-3/11/2011 IEEE.

[4] Young-Chang Hou and Zen-Yu Quan ”Progressive Visual Cryptography with Unexpanded Shares”, Ieee Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 11, November 2011

7695-4994-1/13, 2013 IEEE

[5] “Progressive Visual Cryptography with watermarking for meaningful shares” by JITHI P V, ANITHA T NAIR, 978-1-4673-5090-7/13/ 2013 IEEE.

