International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 7, October 2014, PP 253-259
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

A Review on Cheating Identification and Prevention in Secret Sharing Scheme Using Digital Watermarking

Reshma More
Computer Engineering,
DCOER, Pune, India
reshmam511@gmail.com

Gajanan Wayal
Computer Engineering,
DCOER, Pune, India
wayal14gajanan@gmail.com

Neha Thopte
Computer Engineering,
DCOER, Pune, India
n.smile20@gmail.com

Divya Walgude
Computer Engineering,
DCOER, Pune, India
divya.walgude93@gmail.com

Prof N.J. Kulkarni
Asst. Professor,
Computer Engineering,
DCOER, Pune, India
nikita.kulkarni@zealeducation.com

Prof S.S Mujgond
Asst. Professor,
Computer Engineering,
DCOER, Pune, India
shivganga.mujgond@zealeducation.com

Abstract: *Visual cryptography (VC) is numerous applications, including visual authentication and identification, steganography, image encryption and digital watermarking. A new cryptographic scheme proposed for securing color image based on visual cryptography scheme.The watermark method is an excellent technique to protect the original information of a digital image.In exiting system there is work on binary images.we are introduced new system which are using the sharing schemes for dividing color image and apply digital watermarking for security of shares.We are dividing our system into three main phases creation of shares, distribution of shares and construction of secret.since we are identify and prevent cheater participant and block the cheater participant.In this paper, we and show that it is not cheating immune. We also outline an improvement that helps to overcome the problem.*

Keywords: *Secret sharing scheme, cheating identification and prevention, digital watermarking, visual cryptography (VC).*

1. INTRODUCTION

1.1. Visual Cryptography

Visual Cryptography is a new Cryptography technique which is used to secure the images.In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. Visual cryptography scheme is the concept of encrypting a secret image into n(more than one) shares[7][10].Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns[8].Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns[1].

1.2. Watermarking

The original image containing the watermark pattern is name as “markimage ”.the watermark image method satisfy the transparency and robustness[14].

In this system, we work on color image. We are taking one Secret and dividing that secret into different shares then applies watermarking it with a secret image using DCT algorithm. After that we are going to make n shares from the watermarked image then distribute them into n participants. K Participant will bring the share give dealer for reconstruction of secret. This share will find the watermark stored in database. Then by superimposing these k shares we will get watermarked image generated. Then we will apply Inverse-DCT on watermarked image to check whether shares are valid

or not.if watermark is not match with the database then block the participant. If there is no cheater participant then reconstruct the secret. This application will be used by people working in high security zones like military application, government application for the authentication purpose.

2. AIM

Develop an application which increases the security by sharing secret using visual cryptography by encrypting invisible watermark into shares.

2.1.Related Work

In a visual secret-sharing scheme, the shares given to participants are xeroxed onto transparencies. The main goal of secret sharing is to protect important secret data,such as cryptographic keys ,from being lost or destroyed without accidental exposure[1][2]. The analysis of Otsus threshold method and LSB matching steganography algorithm for addressing the challenging problem of visual quality of embedded shares in cryptography based visual secret sharing system. The proposed method not only increases the visual quality of recovered secret but also gives better results. It also improves the PSNR as compared to other methods[4].A region based visual cryptography scheme deals with sharing of image based upon splitting the image into various regions. The main concept of visual secret sharing scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information about the original image unless all the shares are obtained. The original image is obtained by superimposing all the shares directly, so that the human visual system can recognize the shared secret image without using any complex computational devices. In this paper we propose a region based visual secret sharing scheme for color images with no pixel expansion and high security[5].The color visual cryptography methods are free from the limitations of randomness on color images. The two basic ideas used are error diffusion and pixel synchronization. Error diffusion is a simple method, in which the quantization error at each pixel level is filtered and fed as the input to the next pixel. In this way low frequency that is obtained between the input and output image is minimized which in turn give quality images. Degradation of colors are avoided with the help of pixel synchronization. The proposal of this work presents an efficient color image visual cryptic filtering scheme to improve the image quality on restored original image from visual cryptic shares. The proposed color image visual cryptic filtering scheme presents a deblurring effect on the non-uniform distribution of visual cryptic share pixels. After eliminating blurring effects on the pixels, Fourier transformation is applied to normalize the unevenly transformed share pixels on the original restored image. This in turn improves the quality of restored visual cryptographic image to its optimality. In addition the overlapping portions of the two or multiple visual cryptic shares are filtered out with homogeneity of pixel texture property on the restored original image. Experimentation are conducted with standard synthetic and real data set images, which shows better performance of proposed color image visual cryptic filtering scheme measured in terms of PSNR value (improved to 3 times) and share pixel error rate (reduced to nearly 11%) with existing grey visual cryptic filters. The results showed that the noise effects such as blurring on the restoration of original image are removed completely[8][9].

2.2.Existing System

The visual cryptography was initially introduced and used only on binary images i.e black and white images.

Black and white images are divided into shares but the secret are easily identified from those shares because security is not provided in this scheme. Using digital watermarking we applied the security. In black and white image we are not applied digital watermarking so that security is not provided.

2.3. Drawback of Existing System

- Digital watermarking is not used so security is not provided.
- Cheater cannot identified and prevent easily because watermark technique is not Used

3. PROPOSED WORK

In proposed system, we are making shares of secret and storing them on different participant. This will solve the problem of secret misuse .Visual cryptography is a new technique which provides information security which uses wavelet algorithm. In this technique identification and prevention done by digital watermarking using DCT and IDCT.DCT(Descret Cosine Transform)apply before the

distribution of shares and IDCT(Inverse Descret Cosine Transform)will be applied at the time of reconstruction phase.

3.1. Advantages of Proposed System

- We are not using textual passwords so security is high.
- Secret Distribution into n numbers of participant so Cheater participant cannot access it easily.
- We are providing more security due to watermarking so identification and prevention of cheater participant done easily.
- We are providing a fix size of image and the size shares.

3.2. Modules

3.2.1. Creation of Shares

In creation of shares, use different sharing schemes for e.g. (k,n) and (n,n).we are using (k,n) sharing schemes for creation of shares as shown in fig(a).

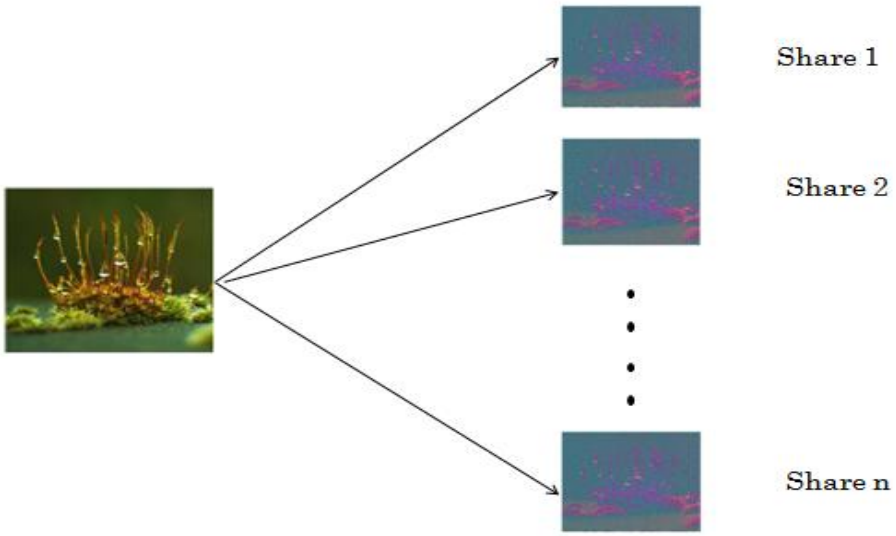
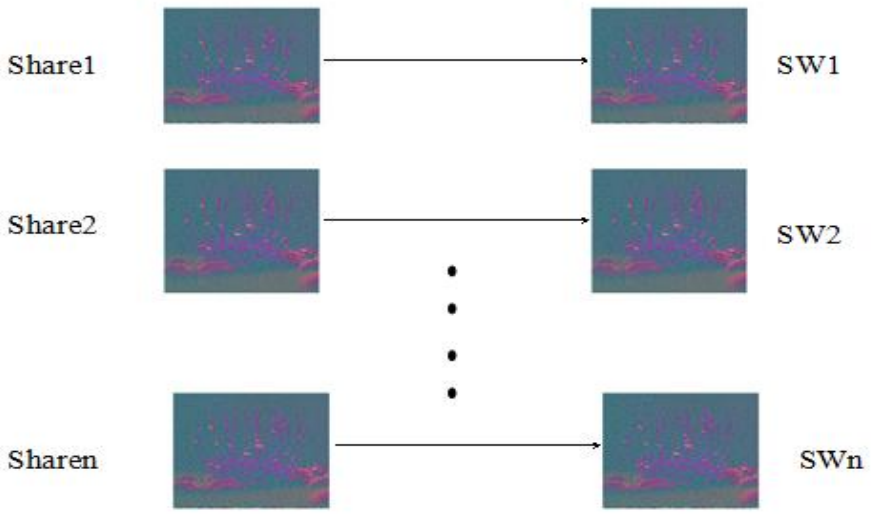


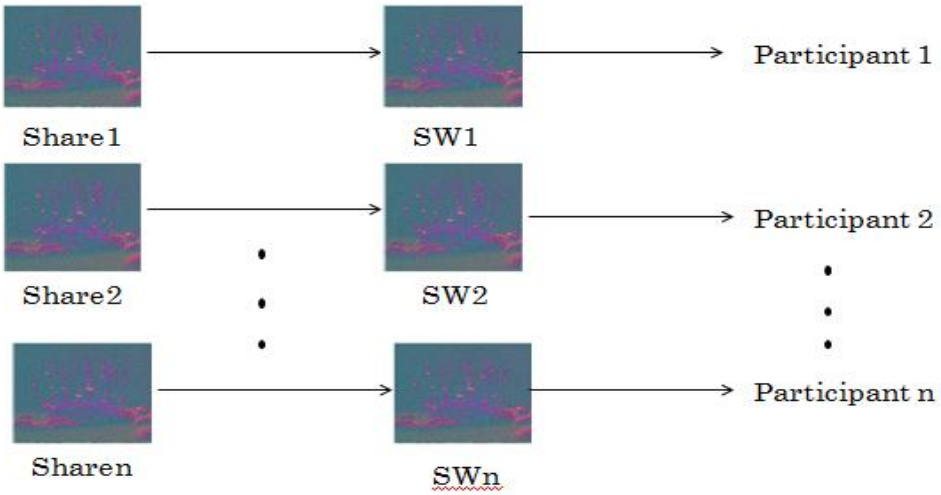
Fig (a). *Creation of shares*

3.2.2. Distribution of Shares

In distribution of shares, we are applying a DCT algorithm on each share of color image as shown in fig (b1) and then distribute those shares to n numbers of participant fig(b2).



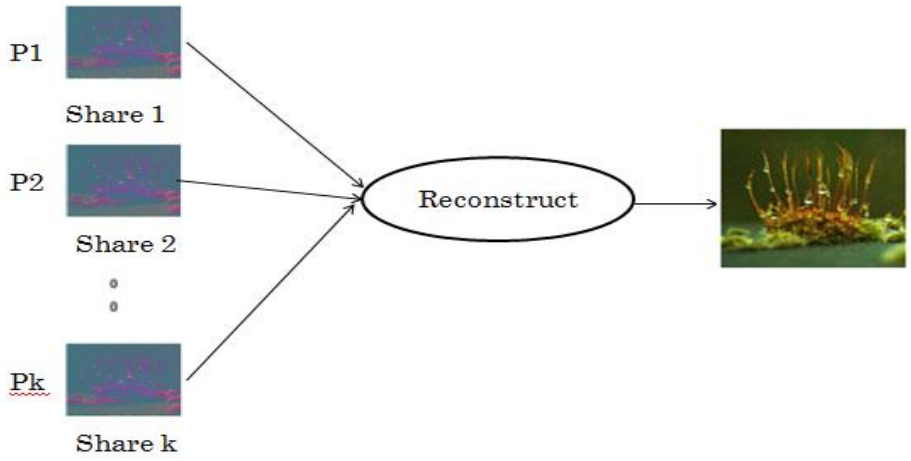
Fig(b1). *Apply Watermark*



Fig(b2). *Distribution of shares*

3.2.3. Reconstruction of Secret

In reconstruction of secret, we are applying a IDCT algorithm on each share and identify the authentic participant and reconstruct the secret as shown in fig(c).



Fig(c).*Reconstruction of secret*

3.3. System Architecture

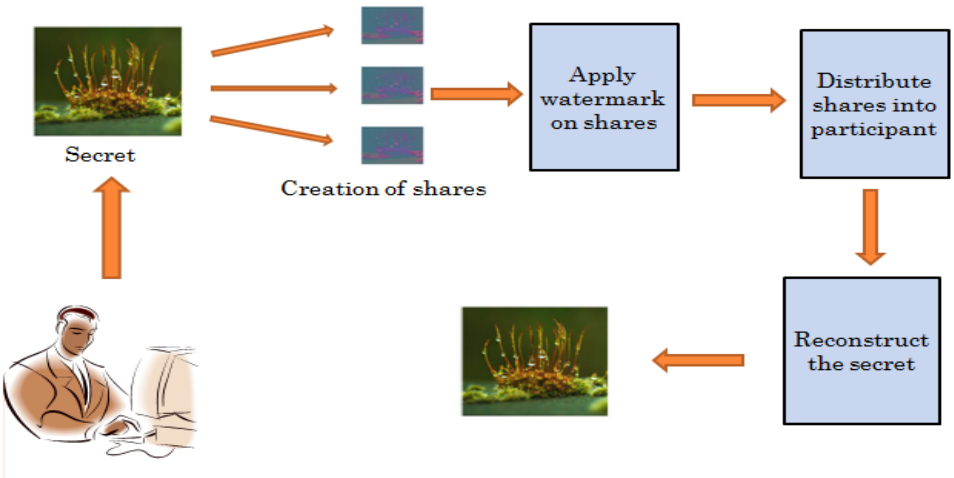


Fig1. *System architecture*

In above fig(1). We are taking one Secret and dividing that secret into different shares then applies watermarking it with a secret image using DCT algorithm. After that we are going to make n shares from the watermarked image then distribute them into n participants. K Participant will bring the share give dealer for reconstruction of secret. This share will find the watermark stored in database. Then by superimposing these k shares we will get watermarked image generated. Then we will apply Inverse-DCT on watermarked image to check whether shares are valid or not.if watermark is not match with the database then block the participant.

3.4. Mathematical Model

1. Let S is the System

   S = {……}

2. Let I is the set of Images

   I = {I1, I2, …. In}

3. Let P is the set of shares

   P= {P1, P2, …. Pn}

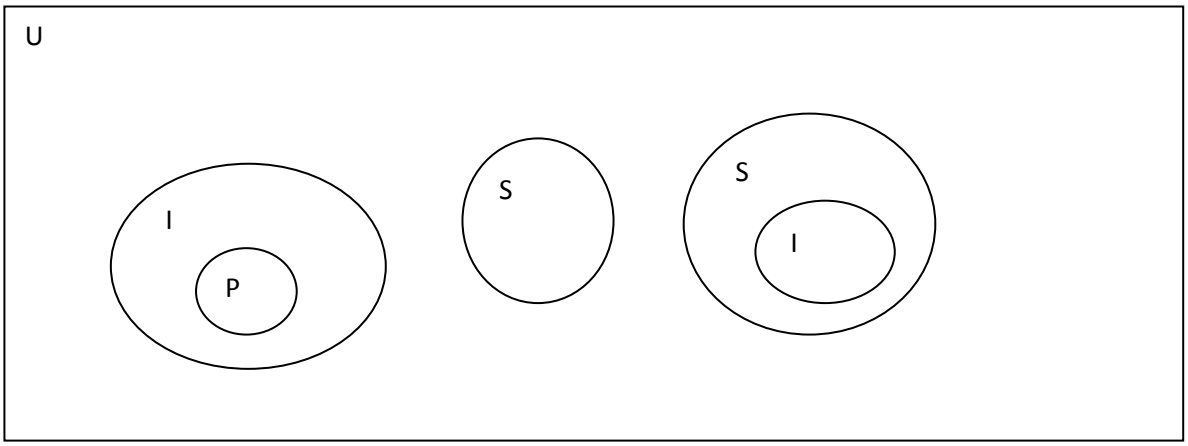
4. Let R is the set of secret images

   R = {R1, R2, … , Rn}

3.5. Mathematical Representation

Here 'S' is the set of complete system

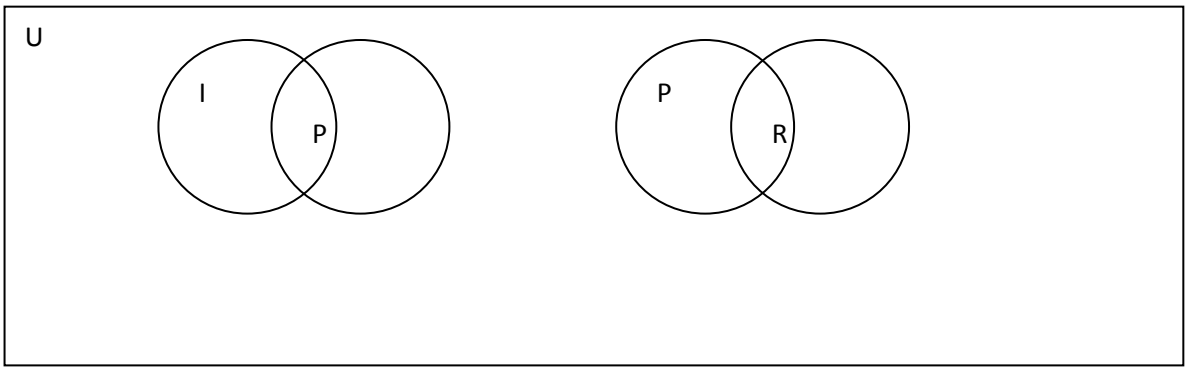
S = {I, P, R}



So now

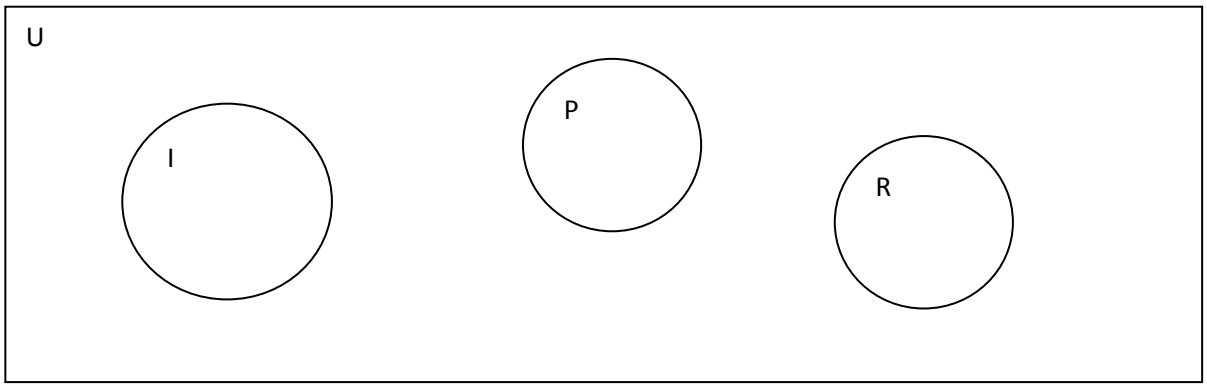
I = { {P} } I = { {P1, P2, P3, Pn} }

S = { {I} } S = { { I1, I2, I3, In} }



Here Set of shares is the union with set of images {I} U {P}

Set of secret images is union with set of shares {P} U {R}



At the authentication phase all sets must match each other in order to complete successful authentication of corresponding person.

U = { {I1, I2, I3, In}, {P1, P2, P3, Pn}, {R1, R2, R3, Rn} }

4. SYSTEM FEATURES

- System will register the user by clicking his picture and generating shares after watermarking. User will get his part of share while registering.
- User will give his part of share in order to get access of the system. System will extract watermark from the generated image to validate the shares.

5. CONCLUSION

Cryptographic schemes are very useful for realizing information security. We have crypt analyzed a cheating prevention and identification scheme in visual cryptography.Secret Distribution into n numbers of participant so Cheater participant cannot access it easily.We are providing more security due to watermarking so iidentification and prevention of cheater participant done easily. We are providing a fix size of image and the size shares.

REFERENCES

[1] E Yu-Chi Chen, Student Member, IEEE, Gwoboa Horng, and Du-Shiau Tsai" Comment on Cheating Prevention in visual cryptography",IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 7, JULY 2012

[2] Gopi Krishnan and Loganathan "Color image cryptography scheme based visual cryptography",ICSCCN 2011

[3] Sagar Kumar Nerella, Kamalendra Varma Gadi and RajaSekhar Chaganti"Securing Images Using Color Visual Cryptography and Wavelets",March 2011

[4] Shital B. Pawar, Prof.N.M.Shahane "Visual Secret Sharing Using Cryptography", Jan. 2014

[5] D.R. Denslin Brabin, Divya Venkatesan, Divyalakshmi Singaravela Lekha SriRajendran "Region Based Visual Cryptography Scheme for Color Images", March 2013

[6] Bernd Borchert"Segment-based Visual Cryptography", 200

[7] Archana B. Dhole*, Prof. Nitin J. Janwe "An Implementation of Algorithms in Visual Cryptography in Images", March 2013

[8] Zhi Zhou, *Member, IEEE*, Gonzalo R. Arce, *Fellow, IEEE*, and Giovanni Di Crescenzo "Halftone Visual Cryptography", AUGUST 2006

[9] Shiny Malar F.R , Jeya Kumar M.K" Error Filtering Schemes for Color Images in Visual Cryptography",2013

[10] B. Dinesh Reddy, V. Valli Kumari, KVSVN Raju, Y.H. Prassanna Raju"Rotation Visual Cryptography Using Basic (2, 2) Scheme", Jan. 2011

[11] P.S.Revenkar,AnisaAnjum "W .Z.Gandhare"Secure Iris Authentication Using Visual Cryptography", (I1CSIS) International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010.

[12] Er.supriya,kinger,"efficient visual cryptography", journal of emerging technologies in web intelligence, vol. 2, no. 2, may 2010.

[13] L. Masek, P Kovesi, "Recognition of human iris patterns for biometric identification". Tech. Rep., The School of Computer Science and Software Engineering, The University of Western Australia.

[14] Ren-Junn Hwang,"A digital copyright protection scheme based on visual crpytography",tamkang jornal of science and engineering,Vol .3.NO.2,PP.97-106(2000)

AUTHORS' BIOGRAPHY

Miss. Reshma Dilip More was done her diploma in computer technology in BVJNIOT from MSBTE Pune and pursuing BE computer from DCOER Pune in Pune University.

Miss Walgude Divya Tanaji was done her diploma in computer technology in Abhinav collage of poly-technique MSBTE Pune and pursuing BE computer from DCOER Pune in Pune University.

Miss Thopte Neha Sham was done her diploma in computer technology in BVJNIOT from MSBTE Pune and pursuing BE computer from DCOER Pune in pune University.

Mr Wayal Gajanan Dhondu completed his 12th from Shri Shivaji High school and junior Collage, lonar and pursuing BE computer from DCOER Pune in Pune University.