International Journal of Computer Applications Technology and Research
Volume 4– Issue 11, 838 - 845, 2015, ISSN:- 2319–8656

Cheater identification in Visual secret sharing schemes using SHA Algorithm and Alpha channel.

Deepika M P
Cochin University of Science and Technology,
Cochin 22, India

A Sreekumar
Cochin University of Science and Technology,
Cochin 22, India

Abstract: Secret sharing or secret splitting refers to methods for distributing a secret among a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together. Individual shares are of no use on their own. Visual secret sharing (VSS) is an alternate form of secret sharing, where the visual information to be shared is distributed /encrypted in such a way that decryption done using Human Visual System. Visual secret is efficient since secret decoding only depends on the human vision system .There are several visual cryptographic schemes to encode the secret image into shares. In these schemes, normally a participant holds one share, and when the participants stack a sufficient number of shares, the secret image /the original image can be reconstructed through the human visual system. As we know where security is enforcing, there will be some provision to spoil the system. So in this case the dishonest participant, aka cheater, can provide a fake share to cheat other participants thereby he may reconstruct the original one and can use the same for any illegal purpose. In this paper, we propose a cheater identification method by adding an extra alpha channel with each share that contains the authentication information related to that particular share. Moreover the proposed scheme can be used with any visual cryptographic scheme to identify the cheaters.

Keywords: Secret Sharing, Visual Cryptography, Alpha Channel, Cheater Identification, SHA

1. INTRODUCTION

Nowadays digitized personal data is common since technology progresses day by day. Even more of emphasis is on data security today than there has ever been. So protecting these types of data in a secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting research problem even more of emphasis is on data security today than there has ever been.

Visual cryptography is very special data security method which provides a very powerful technique by which one secret can be distributed into two or more shares. When shares on transparencies are super imposes exactly together, the original secret can be discovered without any complicated algorithm or computer participation.

In this paper, many types of visual cryptographic schemes are examined, from the very first type of traditional visual cryptography, up to the latest developments including the positive and negative points of the respective schemes. Cheating is possible in visual cryptography because protection of secret sharing participants is not the main concern. Since there is no restriction on the behavior of the participants, any participant, called a cheater, can reveal a forged share on purpose. Cheating identification in visual cryptography is a main thing in such situations. So we propose a method which uses conventional cryptographic hash function to identify the cheater and prevent such participants.

2. VISUALCRYPTOGRAPHIC SCHEMES:

Visual Cryptography is the scheme which can decode concealed secret image without any cryptographic computations. This scheme is very secure and easy to implement. The basic model consists of a printed page of ciphertext (which can be sent by mail or faxed) and a printed transparency (which serves as a secret key).The original text is revealed by placing the transparency with the key over the page with the ciphertext, even though each one of them is indistinguishable from each other. The system is similar to a one time pad in the sense that each page of ciphertext is decrypted with a different transparency. Due to its simplicity, the system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations.

Visual cryptography (VC) is first introduced by Naor and Shamir [1] in 1994, VC is a cryptographic technique which allows visual information (picture, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system.However, it is distinguished from traditional secret sharing technique [2], in that the decryption of an image encrypted by a visual cryptography scheme requires no mathematical computations or knowledge of cryptography. Instead, the original image becomes visible to the naked eye simply by overlaying cipher transparencies – known as shares – created during the encryption process. Naor and Shamir [1] establish visual cryptography as a visual variant of the k out of n secret sharing problem. In this scheme, one wishes to randomly divide a secret amongst a group of n individuals in such a way as to allow any $k < n$ of them (or, in certain cases, only a qualified subset of them), to recover the secret from their individual shares. However, any number of individuals $k^0 < k$ should be prevented from obtaining any information about the original secret by combining their individual shares.

Visual cryptography schemes are typically lossy and produce decrypted images that are often noisy or suffer from diminished contrast and resolution. A number of factors can affect the quality of the resulting decrypted image in a VC scheme. Typically, as the number of shares n is increased, the contrast of the resulting decrypted image worsens. Furthermore, many schemes produce shares in which each pixel of the original image is represented by multiple pixels in each share, diminishing the resolution of the decrypted image.

It can be tempting to think of visual cryptography as a form of Steganography, but it is important to understand the distinction between the two. In Steganography, one seeks to conceal the existence of a message, perhaps by composing the message using invisible ink. By contrast, visual cryptography – like its true cryptographic counterparts – seeks only to conceal the message itself. It is, however, possible to combine Steganography and visual cryptography to produce two benign -looking images that, when superimposed, reveal a third hidden image.

2.1 A (2, 2) Visual Secret Sharing

The simplest VC algorithm was given by Naor and Shamir [1] in their introductory paper on visual cryptography. They presented a 2 out of 2 scheme, in which 2 shares would be generated (n = 2) for each image encrypted, while decryption would require these 2 shares (k = 2) to be super-imposed. At its most basic level, the 2 out of 2 algorithm works by representing each pixel in the original image by 2 pixels in each share. Each pixel in the original image is read and, if a white pixel is encountered, one of the first two rows in Figure 1 is selected with equal probability, and each share is assigned a 2 pixel block as shown in the third and fourth columns. Similarly, if a black pixel is encountered, one of the last two rows is selected with equal probability, and is assigned to each share.

If two white pixels overlap when two shares are superimposed, the resulting pixel will be white. By contrast, if a black pixel in one share overlaps with either a white or black pixel in the other share, the resulting pixel will be black. This implies that the superimposition of the shares represents the Boolean OR functions. The last column in Figure 1 shows the resulting subpixel when the subpixels of both shares in the third and fourth columns are superimposed.

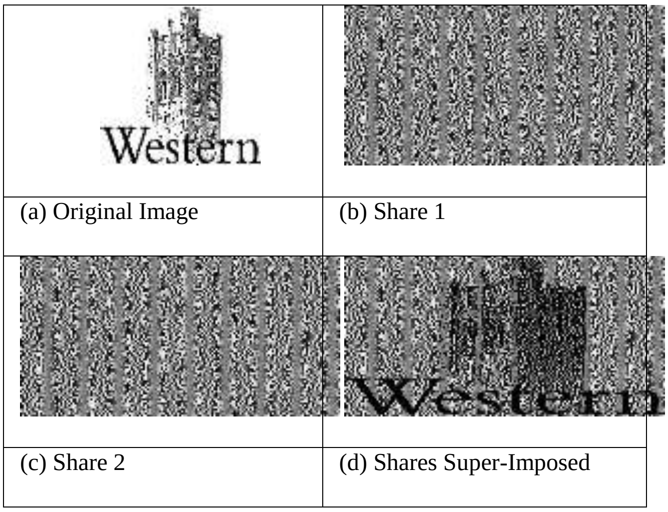
As demonstrated in Figure 1, if a pixel in the original image was black, the subpixel in the superimposition of the two shares will be fully black. Similarly, if a pixel in the original image was white, the subpixel in the superimposition of the two shares will be black and white. However, because the pixels are small and situated very close together, the human eye averages the relative contributions of the black and white pixels, resulting in a grey pixel.

Figure 2 shows the encryption and decryption of the University of Western Ontario logo using Naor and Shamir’s 2 out of 2 algorithm, in which 2 subpixels are used for each original pixel. Neither share generated reveals any information about the original image, but when the two are superimposed as shown in Figure 2(d), a representation of the original image can be seen. The aspect ratio of the original image is distorted in the decrypted version due to the fact that the use of 2 subpixels per original pixel doubles the width of the decrypted image while retaining its original height.

Figure 1: 2 out of 2 using 2 subpixels per original pixel

Original Pixel	Probability	Share 1	Share 2	Super imposed
□	0.5	■□	■□	■□
□	0.5	□■	□■	□■
■	0.5	■□	□■	■■
■	0.5	□■	■□	■■

Figure 2: 2 out of 2 encryption/decryption using 2 subpixels per original pixel



(a) Original Image

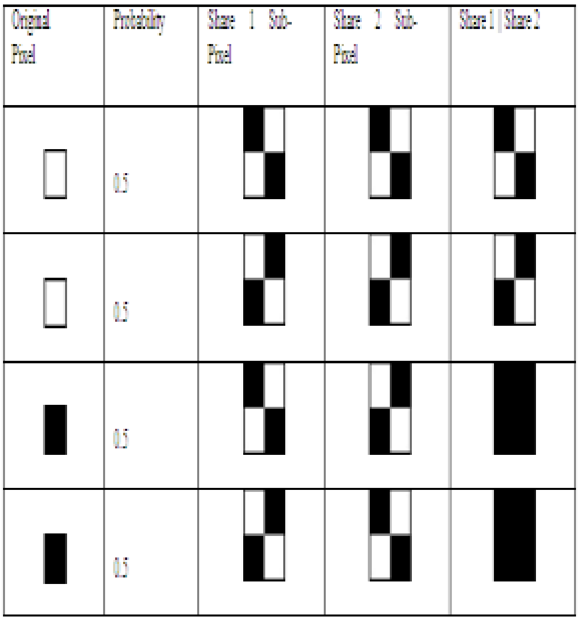
(b) Share 1

(c) Share 2

(d) Shares Super-Imposed

To compensate for the distortion of the aspect ratio of the original image, Naor and Shamir [1] recommend using a 2 × 2 subpixel block to represent each original pixel. This produces an image that is four times the size of the original image, but retains the aspect ratio of the original image. Figure 3 shows the subpixels used in this new variant of the 2 out of 2 algorithm.

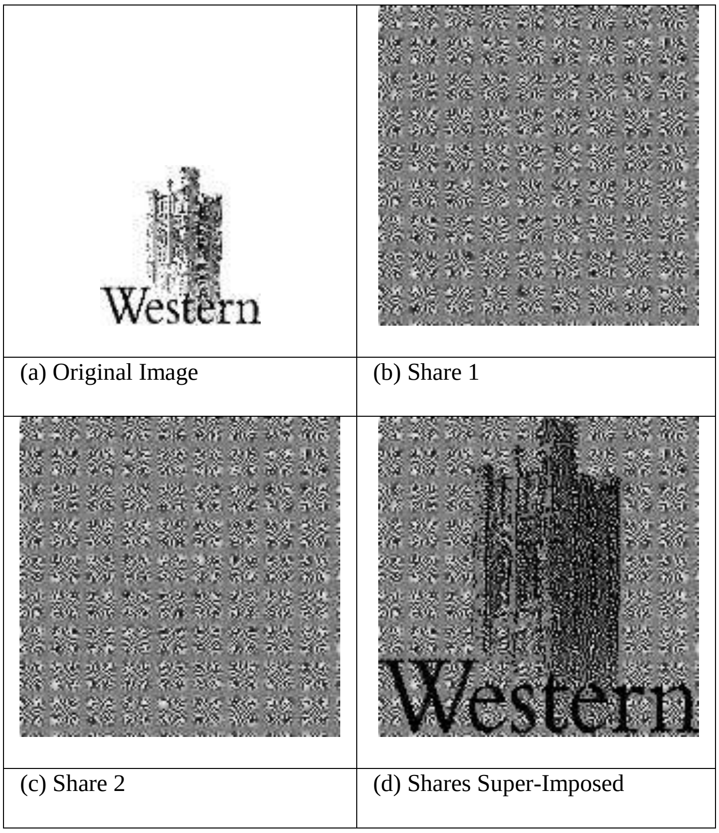
Figure 3: 2 out of 2 using 4 subpixels per original pixel



Original Pixel	Probability	Share 1 Sub-Pixel	Share 2 Sub-Pixel	Share 1 | Share 2
□	0.5	■□ □■	■□ □■	■□ □■
□	0.5	□■ ■□	□■ ■□	□■ ■□
■	0.5	■□ □■	□■ ■□	■■ ■■
■	0.5	□■ ■□	■□ □■	■■ ■■

Figure 4 shows an encryption and decryption cycle on the same image used in Figure 2, this time using the 4 subpixel variant of the 2 out of 2 algorithm. It is clear that while the image is four times as large as the original, its original aspect ratio has been preserved, producing a clearer and more natural looking result.

Figure 4: 2 out of 2 encryption/decryption using 4 subpixels per original pixel



(a) Original Image

(b) Share 1

(c) Share 2

(d) Shares Super-Imposed

2.2 Extended Visual Cryptography:

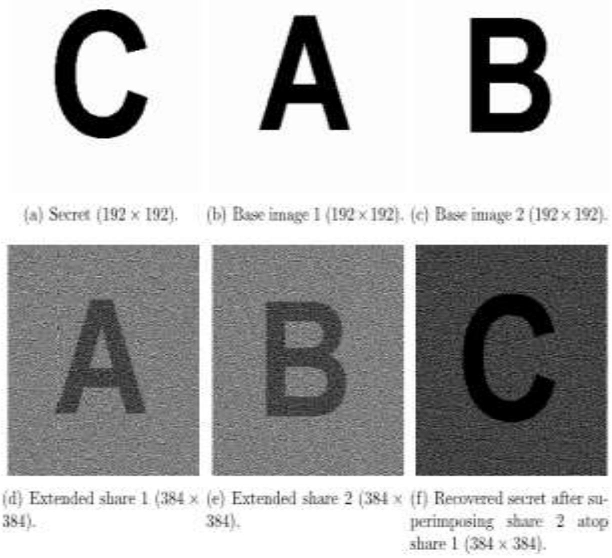
Extended VC takes the idea of visual cryptography further by creating shares which are meaningful to anyone who views them. This helps to alleviate suspicion that any encryption has taken place and also presents visually pleasing shares which incorporate all the previously mentioned features of VC. Extended visual cryptography schemes allow the construction of shares in which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, the meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography.

Figure 5.shows an example of a (2, 2) EVCS. As can be seen from the figure, two meaningful shares are generated from the base images. During this share creation, the secret is encoded between each of the shares. After superimposing each share, the secret is completely recovered while the meaningful information on each share completely disappears.

In order to use this extended visual cryptography scheme, a general construction needs to be defined. Ateniese et al. [19] have devised a mechanism by which we can generate the shares for the scheme. A stronger security model for EVCS is one in which the shares associated with a forbidden subset can be inspected by the user, meaning that the secret image will still remain totally hidden even if all n shares are previously known by the user. A symmetric approach to fully address a general (k, n) problem was also proposed in [19].

For each set of access structure, let $P = \{1,2, \dots . n\}$represents the set of elements called participants, and let 2^P denote the set of all subsets of P. Let $\Gamma_{Qual}/\Gamma_{Forb}$ be the collection of Qualified / Forbidden sets. The pair is called the access structure of the scheme. Any qualified set can recover the shares image by stacking its participant's transparencies, while any forbidden set has no information on the shared image. This extension generalizes the original secret sharing problem by [2]. In [19] the authors propose a new technique to realize (k, n) VCS, which is better with respect to the pixel expansion than the one proposed by Naor and Shamir.

Figure 5: The result of (2, 2) –EVCS encryption process



(a) Secret (192 × 192).

(b) Base image 1 (192 × 192).

(c) Base image 2 (192 × 192).

(d) Extended share 1 (384 × 384).

(e) Extended share 2 (384 × 384).

(f) Recovered secret after superimposing share 2 atop share 1 (384 × 384).

One of the most potentially useful types of visual cryptography scheme is colour visual cryptography. The reason for this is that the majority of people nowadays are more used to colour images and interact with them more frequently. Natural colour images can be used to share secrets; this provides a very helpful cover for unsuspicious hiding the fact that any encryption has taken place at all. However, some of these schemes do not work without a computer, which does defeat the main purpose of visual cryptography. Other colour schemes do try to keep with the main ethos of instantaneous decryption without a computer.

2.3. Colour Visual Cryptography:

Visual cryptography schemes were applied to only black and white images till year 1997. A very primitive example of color image sharing appears in [16].Verheul and Van Tilborg proposed an important color visual cryptography scheme [17]. In this visual cryptography scheme one pixel is distributed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black. In 2000, Yang and Laih [18] proposed a different construction mechanism for the colored visual cryptography scheme. They argued that their method can be easily implemented and can get much better block length than Verheul and Van Tilborg's scheme.

F.Liu, C.K.Wu, X.J. Lin [20] proposed a new approach for colored visual cryptography scheme. They proposed three different approaches for color image representation:

- In first approach, colors in the secret image can be printed on the shares directly. It works similar to basic visual cryptography model. Limitations of this approach are large pixel expansion and quality of decoded image is degraded.
- In second approach separate three color channels are used. Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. Then normal visual cryptography scheme for black and white images is applied to each of the color channels. This approach reduces the pixel expansion but quality of image gets degraded due to half toning process.
- In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image.

A major common disadvantage of the above reviewed colored VCS schemes is that the number of colors and the number of subpixels determine the resolution of the revealed secret image. If many colors are used, the subpixels require a large matrix to represent it. Also, the contrast of the revealed secret image will go down drastically. Consequently, how to correctly stack these shared transparencies and recognize the revealed secret image are the major issues.

Recently, more and more applications of visual cryptography, such as authentication, human identification, copyright protection, watermarking, visual signature checking etc. are introduced. The print and scan application of VCS is also introduced by researchers. In this application, scan the shares into a computer system and then digitally superimpose their corresponding shares. This would make possible secure verification of e-tickets or other documents. The developments and the research works done by other researchers in the different perspectives on visual cryptography, such as access structure, generation of shares and other aspects are already reported by different authors.

3. CHEATING IN VISUAL CRYPTOGRAPHY:

In VC, all participants who hold shares are assumed to be semi-honest, that is, they will not present false or fake shares during the phase of recovering the secret image. Thus, the image shown on the stacking of shares is considered as the real secret image. Nevertheless, cryptography is supposed to guarantee security even under the attack of malicious adversaries who may deviate from the scheme in any way. For cheating, a cheater presents some fake shares such that the stacking of fake and genuine shares together reveals a fake image.

Horng [6] proposed that cheating is possible in (k, n)-V SS where k < n. The cheating activity of Horng is that the n-1 cheaters collusively use their transparencies to know the secret and infer the victim's transparencies T_v; thus they can generate fake transparencies FTs to make the victim to accept the cheating image by stacking FTs + T_v.

Consider (2, 3)-V SS scheme as an example in Figure 6. As secret image is encoded into three distinct transparencies, denoted T_1, T_2, T_3, Then, the three transparencies are respectively delivered to Alice, Bob, and Carol. Without lose of generality, Alice and Bob are assumed to be the collusive cheaters and Carol is the victim. In cheating, $T_1$and T_2 to create forged transparency T_2'such that superimposing T_2' and T_3 will visually recover the cheating image. Precisely, by observing the following collections of 3 × 3 matrices which are used to generate transparencies, the cheaters can predict the actual structure of the victim's transparency so as to create T_2'.

$$\text{Create T2'. } C^{0=}\begin{bmatrix}100\\100\\100\end{bmatrix}\text{and } C^{1=}\begin{bmatrix}100\\010\\001\end{bmatrix}$$

By observing the above matrices, two rows of above C^0 or C^1matrix are determined by the collusive cheaters. Therefore, the structure of each block in T_3 is exact the remaining row. For presenting a white pixel of cheating image, the block in T_2 is set to be the same structure of T_3. For presenting a black pixel of cheating image, the block in T_2 is set to be the different structure of T_3. Figure 1 and Figure 2 Shows the whole cheating process. Shows the cheaters create to change the decoded image. If the block in T_3 is [010], then T_2 is set to be [010] for a white pixel or it is set to be [001] for a black pixel. Formally, the cheaters can construct a sub-base matrix (SBM) by T_1 and T_2 then infer T_3.

Figure 6: Cheating in visual cryptographic scheme.

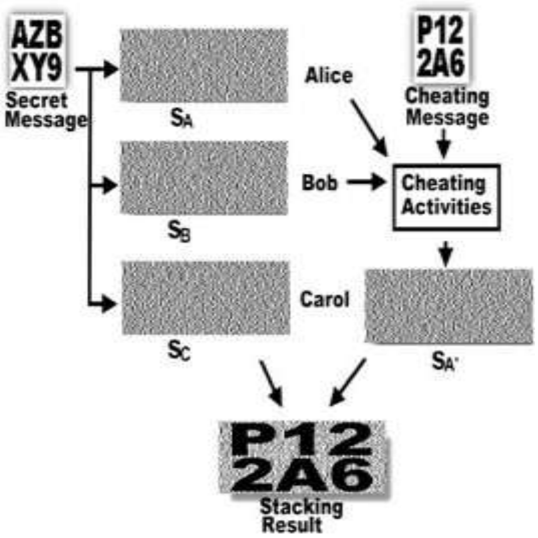
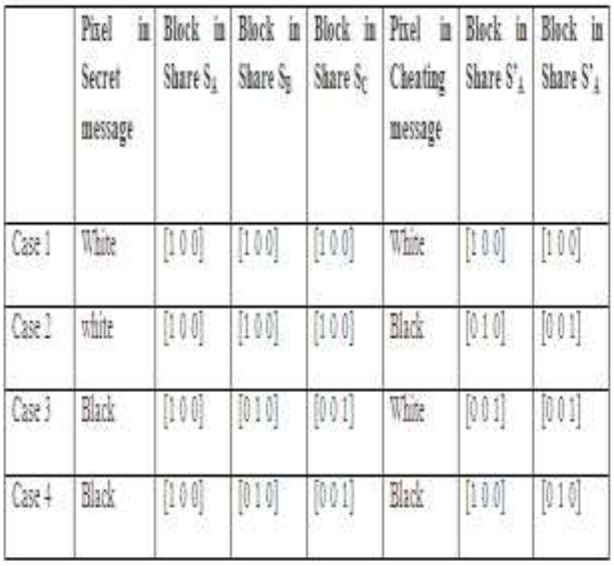


Figure 7.The basic concept of cheating process in 2 out of 3 VCS



	Pixel in Secret message	Block in Share S_1	Block in Share S_2	Block in Share S_3	Pixel in Cheating message	Block in Share S'_1	Block in Share S'_2
Case 1	White	[1 0 0]	[1 0 0]	[1 0 0]	White	[1 0 0]	[1 0 0]
Case 2	white	[1 0 0]	[1 0 0]	[1 0 0]	Black	[0 1 0]	[0 0 1]
Case 3	Black	[1 0 0]	[0 1 0]	[0 0 1]	White	[0 0 1]	[0 0 1]
Case 4	Black	[1 0 0]	[0 1 0]	[0 0 1]	Black	[1 0 0]	[0 1 0]

3.1Cheating Prevention Using Authentication Based

There are several schemes that solves the cheating problem by using verification shares to ensure from other participants are authentic and hence the recovered secrete image is authentic. However each participant is burden with a verification share.

An authentication based cheating prevention scheme consists of shares Si and verification shares Vi. Shares Si are generated by any visual cryptographic scheme. Verification shares Vi, for i =1, 2, . . . ,n, generated by the verification shares generation process are used to verify the correctness of the shares Sj, for j =1, 2, . . . ,n and i !=j . Each participant Pi should provide the dealer with a distinct verification logo Li to be used for verifying the authenticity of other shares. All logos are confidential. The verification shares generation process is based on a 2-out-of-2 VC. Each verification share Vi is divided into n−1 regions, R $_{i,j}$ where 1≤j ≤n, j !=i so that when stacking Vi and Sj the logo Li appears in R $_{i,j}$.

The main limitations in this type of scheme are; each participant, however, was burdened with an extra verification share.VC requires total number of n^2 subpixels in all transparencies and this scheme requires total number of $2n^2$ subpixels. Finally in this scheme there is a possibility to create a forged share without modifying any blocks within the victim's region to pass the verification process when the number of n is becoming large.

In [7] Tsai, Chen, Horng scheme, use Generic Algorithms (GA for short) to solve the cheating problem. The proposed scheme does against the cheating attack in VC. The GA based share construction method provides another direction for creating shares.

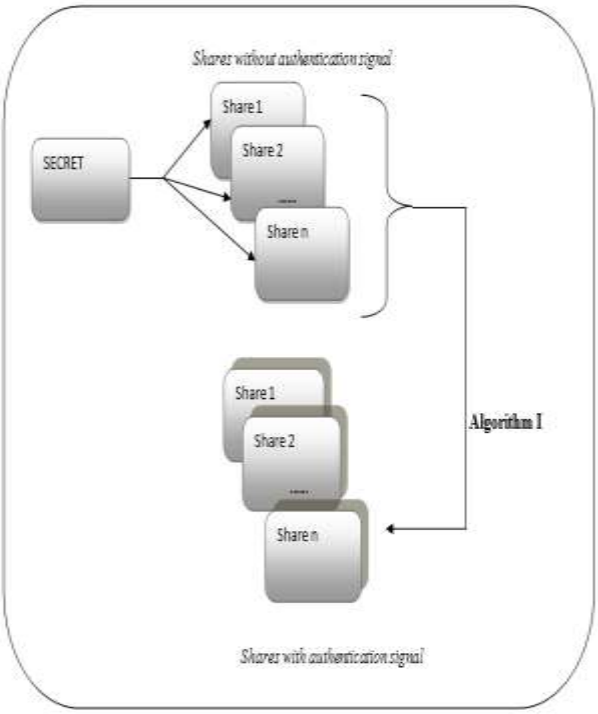
There are different cheating prevention and cheater identification methods in [8][9][10][11][12][13][14], each having its own advantages and disadvantages.

4. PROPOSED METHOD FOR CHEATER IDENTIFICATION:

The proposed method can be used with all kind of secret sharing scheme in visual cryptography. After share construction, using any of the visual cryptographic schemes, an authentication signal is generated for each block(here each raw) of the share using SHA algorithm (Secure Hash Algorithm) and the generated signal is embedded in the alpha channel of the shares. The authentication signal generation phase is described in the Algorithm-I. There are mainly two requirements in the proposed method:

- The size of the secret image as well as shares should be rows *X* 1024.
- The image format of the share should be PNG image. Actually PNG image support alpha channel.

Figure 8. Authentication signal embedding while share construction phase.


Shares without authentication signal
SECRET
Share 1
Share 2
Share n
Algorithm I
Share 1
Share 2
Share n
Shares with authentication signal

Algorithm-I can again used in the generation of authentication signal for each block of the share at reconstruction phase and the generated signal is compared with the authentication signal that is already embedded in the alpha channel of each share. If both signals are same then we can say that the shares are genuine, otherwise fake shares. By this way we can identify that the shares modified or not. While modifying the shares the alpha channel will not be affected.

Algorithm-I

[Each share is having a size *row* × 1024; because in preprocessing stage we are converting the secret image into some size, say *row* × *1024*]

Input: share

Output: share with authentication signal embedded in alpha channel

Step1. Take one row at a time

Step2. For (*i=0* to *row*) do the step 3 and step 4

Step3. Apply SHA- 512 on the bits (*1024*) of the ith row.

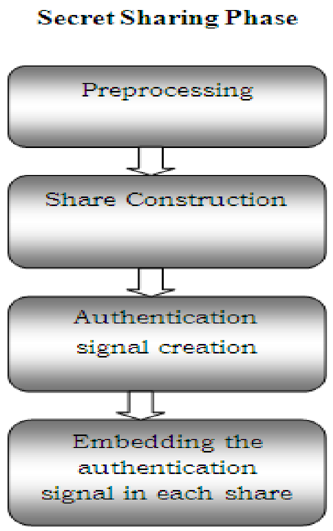
Step4. Resulting *512* bit hash value is embedded as the ith row of alpha channel

Step5. Return the modified share.

Step6. Stop

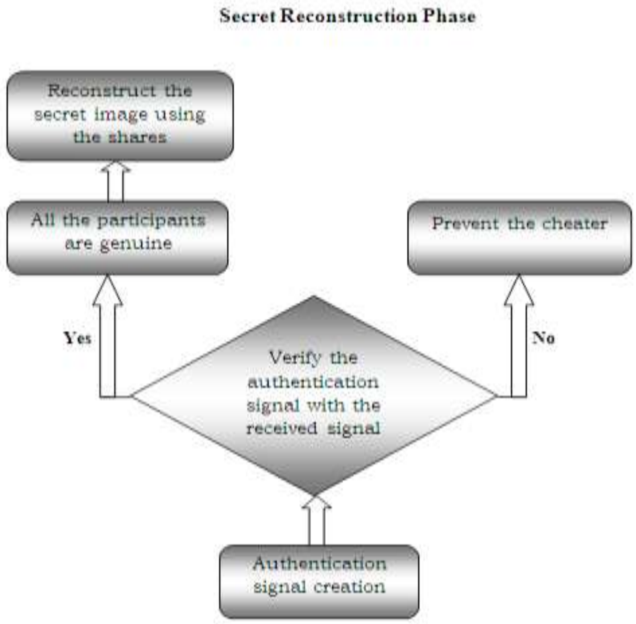
In secret sharing phase the main sub phases are; (a) preprocessing the secret image, (b) share construction (c) Authentication signal creation and (d) Embedding the authentication signal in each share. In preprocessing phase the secret image is converted into the prescribed size, n X 1024 pixels, because the proposed method requires the image to be in n X 1024 pixel size. This makes the application of the SHA -512 algorithm for generating the authentication signal simpler. In the second phase, share construction, any size invariant secret sharing scheme can be used. One of the most important things that should be considered here is the formats of the shares. It should be in PNG image format, because the PNG image format provides the transparent channel called alpha channel with the image. In the proposed system we have used the progressive visual cryptography [4][5] as well as size invariant (2, 3) VCS. In the next phase, by using SHA-512 algorithm generate the authentication signal as prescribed in algorithm 1. And finally embed the authentication signal in the alpha channel of each share and distribute the shares in to the participants.

Figure 9: Secret Sharing Phase


Secret Sharing Phase
Preprocessing
Share Construction
Authentication signal creation
Embedding the authentication signal in each share

The Algorithm II describes the process of secret reconstruction. In the secret reconstruction phase, the proposed system uses the SHA -512 algorithm to find out the authentication signal of each share once again. Then the generated authentication signal is verified against the received authentication signal with each share in alpha channel. If the share is a fake share then the generated authentication signal (using the SHA- 1 algorithm) then the verification fails and the cheating can be identified and prevented at this point.

Figure 10: Secret Reconstruction Phase


Secret Reconstruction Phase
Reconstruct the secret image using the shares
All the participants are genuine
Prevent the cheater
Yes
No
Verify the authentication signal with the received signal
Authentication signal creation

Algorithm-II

[Each received share is having a size *row* × 1024;]

Input: received shares

Output: whether the received share is fake share or not.

Step1. Take one row at a time of received shares having size *row* x 1024.

Step2. For (*i=0* to *row*) do the steps 3, step 4 and step 5.

Step3. Apply SHA- 512 on the bits (*1024*) of the ith row.

Step4. Compare the Resulting 512 bit hash value with the 512 bit that is embedded in the ith row of alpha channel.

Step5. If both 512 bit hash values are not matching then exit the loop by return the share as fake share and go to the step 7, else continue.

Step6. Return the share as the genuine one.

Step7. Stop

5. SECURITY ANALYSIS:

The security of the proposed method directly depends on the strength of the SHA- 512 algorithm. Suppose a single pixel value changed from 0 to 1 for any of the shares, then the number of bit positions that differ between the authentication signal generated in reconstruction phase and the authentication signal generated in the secret sharing phase is 253, almost the half the bit positions of the authentication signal (of 512 bits), indicating that SHA-512 has a good avalanche effect.

6. CONCLUSION:

In this paper, a novel method for cheater identification in the secret sharing schemes is presented. The most important advantage of this method is, it is applicable for all the secret sharing schemes. And the secret analysis shows that even if a single pixel is modified in any of the shares then the authentication signal generated using SHA 1 will be different for that share, and that will lead to the identification of the cheater.

7. REFERENCES

[1]M.Naor, A. Shamir, Visual cryptography, in: Proceedings of the Advances in Cryptology, Eurocrypt ’94, in: LNCS, vol.950, 1995, pp.1–12.

[2].A. Shamir, _How to share a secret,_ Communications of the ACM, vol. 22, no. 11, pp.612_613, 1979.

[3].P.S.Revenkar, Anisa Anjum, W .Z.Gandhare,_ Survey of Visual Cryptography Schemes _International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010

[4]Duo Jin, WeiQi Yan, and Mohan S. Kankanhalli. Progressive color Visual Cryptography. SPIE journal of Electronic Imaging, 14(3), 2005.

[5] 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.

[6]G.Horng,T.H.Chen,D.S.Tsai,Cheating in visual cryptography, Des Codes Cryp-togr.38(2)(2006)219–236

[7]D.S.Tsai ,T.H.Chen ,G.Horng ,A cheating revention scheme for binary visual cryptography with homogeneous secret images ,Pattern Recogn .40(8) (2007) 2356–2366.

[8]C.M.Hu,W.G.Tzeng,Cheating prevention in visual cryptography, IEEE Trans.Image Process.16(1)(2007)36–45.

[9] R.DePrisco,A.DeSantis,Cheating immune threshold visual secret sharing ,Comput. J.53(2010)1485–1496.

[9] Y.C.Chen,G.Horng,D.S.Tsai,Cheating prevention visual cryptography ,Visual Cryptography and Secret Image Sharing,CRCPress,ISBN 9781439837214, 2012

[10] Y.C.Chen,D.S.Tsai,G.Horng,A new authentication based cheating prevention scheme in Naor–Shamir’s visual cryptography ,J.Vis.Commun.Image Repre-sent.23(8)(2012)1225–1233.

[11] Y.C.Chen,G.Horng,D.S.Tsai,Comment on “ Cheating prevention in visual cryp-tography ”,IEEE Trans. Image Process. 21(7)(2012)3319–3323.

[12] Y.C.Chen,D.S.Tsai,G.Horng,visual secrete sharing with cheating prevention revited.,digital signal processing 23 (2013)1496-1504.

[13] Du-Shiau Tsai,Tzung-Her Chen,Gwoboa Horng,Acheating prevention scheme for binary visual cryptography with Homogeneous secret images,pattern rcognition 40 (2007) 2356 – 2366.

[14] C.S Tasai,H.C.Wang,H.C Wu,C.H.M Wang ,”A Cheating –Preventing Visual Cryptography Scheme By Referring The Special Position”, International Journal Of

Innovative Computing ,Information And Control volume 7 , N Umber 7(A),July 2011.

[15]Giuseppe Ateniese,carlo Blundo,Alfredo De Santis, and Douglas R. Stnson. Extenede schemes for visual cryptograpgy. Theoretical Computer Science,250:116,June 1996.

[16]V.Rijmen and B.Preneel. Efficient color Visual encryption for colors of Benetton. ERCRYPTO 96, 1996.

[17]Eric R Verheul and Henk C A Van Tilborg. Constructions and properties of k out of n visual secret sharing schemes.Design Codes Cryptography, 11(2):179–196,1997.

[18]ChingNung Yang and Chi Sung Laih.new colored visual secret sharing schemes.Designs,Codes and Cryptography,20(3):325 –336,2000

[19] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, “Visual cryptography for general access structures”, Proc.ICAL96, Springer, Berlin, 1996, pp.416-428.

[20] [17] F. Liu, C.K. Wu, X.J. Lin, “Colour Visual Cryptography Schemes”, IET Information Security, vol. 2,No. 4, pp 151-165, 2008.

.