Asian Journal of Information Technology 15 (15): 2656-2662, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Color Visual Cryptography Scheme for Natural Images Using Complement Cover and Share Authentication

[1]R. Ramesh Kumar and [2]S. Chandramathi
[1]Department of Computer Science and Engineering, SCAD Institute of Technology, Palladam, Tamil Nadu, India
[2]Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamil Nadu, India

Abstract: Visual cryptography is the method of encrypting secrets in the form of images and reproducing two or more images called shares; the shares on their own do not reveal any secret information. The secret image is reconstructed by stacking the share images manually without any electronic gadgets. Recent researches in visual cryptography are focused towards encrypting color images and embedding the shares into natural cover images which will hide the randomness of traditional shares. Need for verifying the authenticity of the share images used during reconstruction is vital as an inauthentic share will entirely modify the final output. In this study, half toned complement cover share and 2×2 block embedding have been employed to improve the quality of both the share images and the stacked output image. The algorithm also provides a means for verifying the authenticity of shares sans any additional shares. Experimental results of the proposed work shows better improvement than literature.

Key words: Complement shares, block embedding, verification code, dual embedding, randomness

INTRODUCTION

Even with the incredible innovation of computer technology, using a computer to decrypt secrets is not feasible in some situations. For example, a computer dependent decryption technology would become absolutely inadequate in locations lacking computing facility or with end-users lacking the necessary computer knowledge. In these situations, most reliable and convenient method for verification and secret recovery is the human visual system. Visual Cryptography (VC), proposed by Naor and Shamir (1995) is a method for protecting image-based secrets without the requirement of complex algorithm for decryption. In their (2, 2) VC scheme each secret image is encrypted into two shares such that no information can be retrieved from any single share. Shares are printed in transparent sheets and by stacking the two shares the secret image can be visualized by naked eye without any complex cryptography algorithms. In the above basic VC scheme, each pixel of the secret image is encrypted on a two pixels per share basis. If the input pixel is white, one of the two columns under the white pixel in Fig. 1 is chosen. If the input pixel is black, one of the two columns under the black pixel is chosen. In each case, the choice is performed randomly such that each column has a 1/2 probability of being chosen. Then, the first two pairs of pixels in the selected column are assigned to share image 1 and the next two to share image 2. Since, in each share image, pixels are encrypted into a black white or white black pair of pixels, an individual share image gives no clue about the input secret image.

Decryption happens by stacking the two share images as shown in the last row of Fig. 1. When stacked, a white pixel of the secret image is depicted by a pair of black and white pixels and a black pixel of the secret image is depicted by a pair of black pixels, irrespective of which column of the pixel pairs was chosen during encryption.

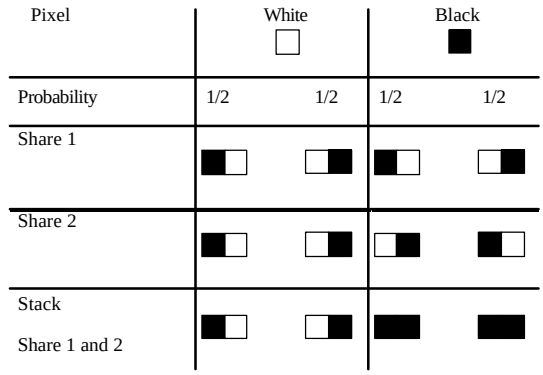

Fig. 1: Visual Cryptography basic scheme

Corresponding Author: R. Ramesh Kumar, Department of Computer Science and Engineering, SCAD Institute of Technology, Palladam, Tamil Nadu, India

Hence, there is a contrast loss in the reconstructed secret image. However, the decrypted secret image is visible to normal eye since human visual system averages their individual black white group. The important parameters of this scheme are:

- Pixel expansion 'm' which refers the number of pixels in a share image used to encrypt a pixel of the secret image. This implies loss of resolution in the restored secret image
- Contrast 'α' which is the relative difference between black and white pixels in the restored secret image, which indicates the quality of the restored secret image

Generally, a smaller value of 'm' indicates a reduction in loss of resolution and a higher value of 'α' indicates an increase in quality of the restored secret image. But, a reduction in 'm', though desired would result in security concerns. So, investigation is concentrated on two paths:

- To ensure quality of restored secret image
- To improve security with minimum pixel expansion

The initial investigations in this field involved only binary and gray scale images. But, of late researchers have also started working with color images. Two main current issues of visual cryptography are the randomness of the share and authenticity of the same. This study, proposes a method that deals with both these issues in color visual cryptography.

Related color visual cryptography schemes: Visual cryptography for color images was first introduced by Naor and Shamir (1996) based upon cover semi groups. Their method can encrypt images with less than two colors only. Rijimen and Preneel presented a 2-out-of-2 VC scheme by applying the idea of color mixture. It supported up to 24 colors and stacking of two transparencies with different colors resulted in a third mixed color. Verheul and Tilborg (1997) introduced the (k, n) visual cryptography schemes for color images scheme. Pixel expansion was high in their scheme. Hou (2003) proposed three schemes for color shares by applying halftone methods and color decomposition. Hou algorithms were for subtractive model and the secret color image is decomposed into yellow, magenta and cyan halftone images.

He then devised three colored (2, 2) color visual cryptography schemes which follow the subtractive model for color mixture by using the existing binary basic visual cryptography scheme. In all the schemes discussed above the reconstructed colors were interpreted by some combination of color mixtures and they generate meaningless shares. Most of visual cryptography methods suffer from a severe limitation which hinders the objectives of visual cryptography.

The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, thereby making the encryption a public fact. The concept of constructing meaningful shares instead of random ones was introduced by Nakajima and Yamaguchi (2002), in their extended visual cryptography scheme for natural images. The shares produced in this method are of very poor quality which again increases the suspicion of existence of secret. Kang *et al.* (2011) proposed color visual cryptography using error diffusion. They tested their algorithm with text input. After thorough analysis of the literature, in this study we propose algorithms for (2, 2) color visual cryptography, the results of which are comparatively better and two more algorithms were proposed which addresses the issue of authenticating the shares.

Proposed method for encryption and embedding color visual cryptography scheme using complement cover image and 2×2 block embedding: In this study, an input RGB secret image is encrypted into two color share images which do not reveal the secret when viewed individually. To avoid the randomness of the shares, one share is encoded into halftoned cover image called MSI (Meaningful Share Image) and the second share is encoded into the halftoned complement of the same cover image called MSI^C (Meaningful Share Image Complement). 2×2 block embedding is used to create MSI and MSI^C.

Generation of MSI and MSI^C: A secret image of dimension nxn is encrypted into two color shares of size m×m where m = 2 n and encoded into cover images of size mxm. The size of the cover image is retained as it is throughout the process. Floyd halftoning (Kang *et al.*, 2011) method is applied for all the three color channels of both the secret image and cover images so that traditional cryptography can be applied. Complement of the cover image is used as the second cover which eliminates the interference of the cover image during decryption, i.e., a normal cover when stacked with its complement cover gets negated thereby eliminating any possibility of interference by the cover images. In this study, we propose an algorithm for meaningful share generation

using complement cover image which secures RGB natural secret image. The process of generating meaningful shares is explained in algorithm 1.

Algorithm 1: Generation of meaningful shares:

Input: color image of size $n \times n \rightarrow SI_{(n,n)}$
cover image of size $m \times m \rightarrow CI_{(mxm)}$ where m=2n
Output: meaningful shares of size $m \times m \rightarrow MSI_{(mxm)}, MSI^{C}_{(mxm)}$
Begin
Step 1 : Split the images into 3 color channels.
$SI_{(n,n)} \rightarrow \{ SI_{(R)}, SI_{(G)}, SI_{(B)} \}$
$CI_{(m,m)} \rightarrow \{ CI_{(R)}, CI_{(G)}, CI_{(B)} \}$
Step 2 : Error diffusion for $SI_{(R)}$
Threshold→T
$hSI_{R(mxm)} = 0$
$ER_R = 0$
for rows = 1 to m-1,
$hSI_R(rows,1) = 255*(if(SI_R(rows,1) = T))$
$ER_R = - hSI_R(rows,1) + (SI_R(rows,1)$
Apply error diffusion with the filter
$P_i = \frac{1}{16} P_{i-1} P^{i}_{5} 7 \quad \forall SI_R(rows,1)$
for cols = 2 to n-1
$hSI_R(rows,cols) = 255*(if(SI_R(rows, cols) = T))$
$ER_R = - hSI_R(rows, cols) + (SI_R(rows, cols)$
Apply error diffusion with the filter
$P_i = \frac{1}{16} P^{i-1}_{3} P^{i}_{5} {}^{7}_{1} \quad \forall SI_R(rows,cols),$
end
$hSI_R(rows,n) = 255*(if(SI_R(rows,n) = T))$
$ER_R = - his_R(rows,n) + (SI_R(rows,n)$
Apply error diffusion with the filter
$P_i = \frac{1}{16} P^{i-1}_{5} P^{i}_{-} {}_{-} \quad \forall SI_R(rows,n),$
end
rows = m
$hSI_R(rows,1) = 255*(if(SI_R(rows,1) = T))$
$ER_R = - hSI_R(rows,1) + (SI_R(rows,1)$
Apply error diffusion with the filter
$P_i = \quad \forall SI_R(rows,1),$
for cols = 2 to n-1
$hSI_R(m,cols) = 255*(if(SI_R(m,cols) = T))$
$ER_R = - hSI_R(m,cols) + (SI_R(m,cols)$
Apply error diffusion with the filter
$P_i = \frac{1}{16} P^{i-1}_{-} P^{i}_{-} {}^{7}_{-} \quad \forall SI_R(rows,1),$
end
Step 3 : Repeat step 2 ? $SI_{(G)}, SI_{(B)}, CI_{(R)}, CI_{(G)}, CI_{(B)}$
Step 4:∀pixels $P_{(i,j)}$ of $hSI_{R(nxn)}$, $hSI_{G(nxn)}$, $hSI_{B(nxn)}$, $hCI_{R(mxm)}$, $hCI_{G(mxm)}$, $hCI_{B(mxm)}$
i =1 to n,m & j= 1 to n,m
$P_{(i,j)} = 1*(if(P_{(i,j)} = T))$
Step 5 : $hCI^{C}_{R} = \sim hCI_R$
Step 6 : repeat step 5∀hCI_G, hCI_B
Step 7 : Encryption & Embedding
for each 2×2 block of hCI_R and hCI^{C}_{R}
for i= 1 to n
for j=1 to n
$\forall hSI_{R(I,j)} = 0$
$hCI_{R(2i,2j-1)}$ & $hCI_{R(2i,2j)}$= perm{01,10}
$hCI^{C}_{R(2i,2j-1)} = hCI_{R(2i,2j-1)}$
$hCI^{C}_{R(2i,2j)} = hCI_{R(2i,2j)}$
$\forall hSI_{R(I,j)} == 1$
$hCI_{R(2i,2j-1)}$ & $hCI_{R(2i,2j)}$= perm{01,10}
$hCI^{C}_{R(2i,2j-1)} = hCI_{R(2i,2j-1)}$
$hCI^{C}_{R(2i,2j)} = hCI_{R(2i,2j)}$
end
end
Step 8 : Repeat step 7 ? (hCI_G, hCI^{C}_{G}) and (hCI_B, hCI^{C}_{B}) using hSI_G, hSI_B respectively.
Step 9 : Share 1 $MSI_{(mxm)}$ = cat (hCI_R, hCI_G, hCI_B)
Step 10 : Share 2 $MSI^{C}_{(mxm)}$ =cat($hCI^{C}_{R}, hCI^{C}_{g}, hCI^{C}_{B}$)
end

The algorithm starts by separating the secret and cover images into individual color channels and each channel is error diffused using Floyd halftonning method. Each halftoned channel is converted into single tone using a threshold 'T'. In continuation each pixel of the halftoned secret image is processed channel wise and encrypted using 2×2 visual cryptography technique. Then, the encrypted pixels are embedded into the halftoned cover image and the complement of the same cover image on a two pixels per cover basis. Most of the literature have used different natural image for cover images which in turn have results in interference of the cover images in the final stacked output. In our method since we use an image and its complement as cover images the effect of interference while stacking is nullified and a common black background is formed for better projection of the output. For embedding the pixels into the cover images (Kang *et al*., 2011) have identified VIP (Visual important pixels) in the cover images and retained the same value and position in the cover images and the encrypted secret pixels is embedded into the remaining pixels. They are retaining only one pixel of the cover image for each 4 pixels of the encrypted secret image which reduces the quality of the meaningful shares. Also they have tested only for text images. In our method we have concentrated on the quality of the both the meaningful shares and the stacked output. Here instead of VIP we have given importance to SP(secret Pixel) and each pair of SP is embedded into a 2×2 block of both the cover image and the complement cover image. The position of embedding the SP is explained in the algorithm1. Experimental results have shown good improvement than in the literature which is explained in section V.

Decryption: The main advantage of visual cryptography is that it doesn't need any separate complex algorithm for decryption. Just stacking the meaningful shares reveals the secret input image. Human visual system decrypts the output. Hence, this system can be used in places where we can't use a computer or where the involved personnel lack computer knowledge. For testing purpose we have taken bitwise OR of the meaningful shares to see the output which is similar to human visual perception. Sample output of algorithm1 is shown in Fig. 2.

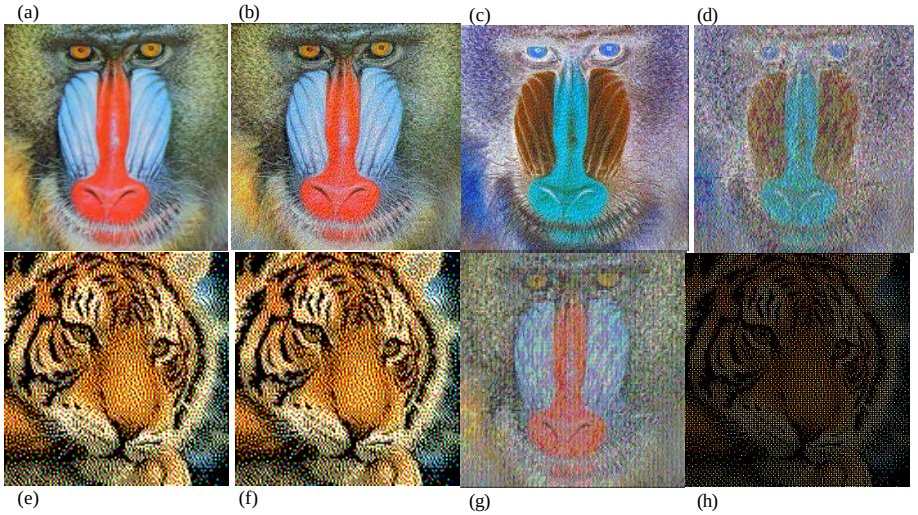

Fig. 2: Sample output for algorithm 1: a) Input Cover Image-CI; b) Secret Image-SI; c) Halftoned Input Cover; d) Halftoned Secret Image-hCI Image-hSI; e) Complement Image-hCI^c; f) Halftoned Share-MSI; g) Complement Share -MSI^c; h) Reconstructed secret

MATERIALS AND METHODS

Proposed methods for share authentication

Share authentication using dual embedding: Most of the literature is built on the assumption that the shares stacked by all the participants are original version of shares. They have not dealt with the possibility of intentional introduction of fake shares. Participants may try to cheat by stacking fake shares generated (Hu and Tzeng, 2007) by different inputs so that the final stacked output may vary. In this study, two methods for authenticating the shares are proposed. A private key as agreed among the participants is generated as color image with white background and the private key is embedded into meaning shares generated by algorithm1. Two different methods are proposed in this section which deals with identification of fake shares without any additional share as in Hu and Tzeng (2007).

Method 1: In (2, 2) Color visual cryptography proposed in section III 50% of the original pixel of the cover images are replaced with the expanded secret pixels. In this method the private key of size n/2 is generated with a white background.

The same technique used in algorithm1 is used to dual embed the private key. The difference is instead of 2×2 block a pair of pixels is embedded into 4×4 block of MSI and MSI^C generated by algorithm 1. In order to retain the quality of the share images and the stacked output one pixel position is selected from the position where secret image is embedded and the next from the remaining 50% of the retained cover image pixels. Alogorithm 2 gives detail about the exact position where the pixels are encoded.

Algorithm 2: Embedding private key into meaningful share:

Input: output of algorithm 1 _$MSI_{(mxm)}$, $MSI^C_{(mxm)}$
Verification signature image of size qxq _ $VI_{(qxq)}$ where q=n/2

Output: meaningful shares of size mxm_$MSI^V_{(mxm)}$, $MSI^{VC}_{(mxm)}$

Begin
Step 1 : Split the images into 3 color channels.
$VI_{(q,q)}$ _{ $VI_{(R)}$, $VI_{(G)}$, $VI_{(B)}$ }
$MSI^V_{(mxm)}$_{ $MSI^V_{(R)}$, $MSI^V_{(G)}$, $MSI^V_{(B)}$ }3
$MSI^{VC}_{(mxm)}$_{ $MSI^{VC}_{(R)}$, $MSI^{VC}_{(G)}$, $MSI^{VC}_{(B)}$ }
Step 2: Do step 2 to 4 of algorithm 1 ? $VI_{(R)}$, $VI_{(G)}$, $VI_{(B)}$
Step 3:Dual Embedding
for each 4x4 block of MSI_R and MSI^V_R,
for i= 1 to n
for j = 1 to n
$\forall$ $VI_{R(I,j)}$ ==0
$MSI_{R(2i,4j-2)}$ & $MSI_{R(2i,4j-1)}$= perm{01,10}
$MSI^C_{R(2i,4j-2)}$= ~ $MSI_{R(2i,4j-2)}$
$MSI^C_{R(2i,4j-1)}$= ~ $MSI_{R(2i,4j-1)}$
$\forall$ $VI_{R(I,j)}$ ==1
$MSI_{R(2i,4j-2)}$ & $MSI_{R(2i,4j-1)}$= perm{01,10}
$MSI^C_{R(2i,4j-2)}$ =$MSI_{R(2i,4j-2)}$
$MSI^C_{R(2i,4j-1)}$ = $MSI_{R(2i,4j-1)}$
end
end
end
Step 4 : Repeat step 7 ? (MSI_G, MSI^C_G) and (MSI_B, MSI^C_B) using VI_G, VI_B respectively.
Step 5 : Share 1 $MSI^V_{(mxm)}$ = cat (MSI_R, MSI_G, MSI_B)
Step 6 : Share 2 $MSI^{VC}_{(mxm)}$ =cat(MSI^C_R, MSI^C_g, MSI^C_B)
end

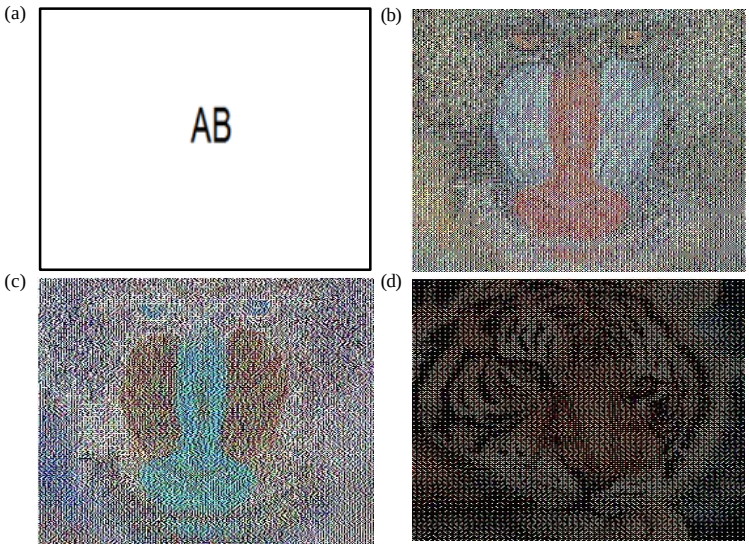

Fig. 3: Sample Output for algorithm 2: a) Verification Image-VI; b) share with verification MSIv; c) Compliment share with d) Reconstructed output with verification MSI^{vc} verification in background

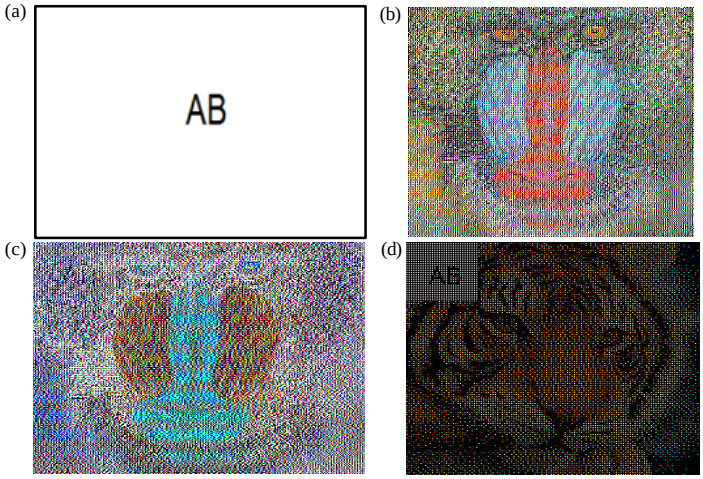

Fig. 4: Sample Output for Algorithm 2; a) Verification Image-VI; b) share with verification MSIv; c) Compliment share with; d) Reconstructed output with verification MSI^{vc} verification in top Corner

This process generates MSI^{V} and MSI^{VC} meaningful shares which have the capacity of verifying the shares. Due to the block size we can visualize the verification image in the background of the stacked output without much reduction in the visual quality of the secret image. And, also by viewing the verification image the share used for decryption is authenticated by all the users. Here, output quality of both meaningful shares and the stacked output get reduced slightly because of dual embedding of the verification private key. But, still the compromise in the quality is acceptable as the algorithm succeeds in verifying the integrity of the shares without any additional shares. Experimental results have shown good improvement than in the literature. Sample output of algorithm 2 is shown in Fig. 3.

Method 2: This section discusses a second method for authentication of share images. During reconstruction in method I the Private Key converted as verification image is seen at the background of the secret image. Method II can be used for verification in situations where the presence of the verification image in the background is deemed a hindrance. Here, we have dual embedded the verification image of size n/4 at any one corner of the share image. Also, the block size is retained as in algorithm 1. During reconstruction the verification image will be present in anyone of the corners. The sample output of algorithm 3 is shown in Fig. 4.

Algorithm 3: Embedding private key in top corner:

Input: output of algorithm 1¬$MSI_{(mxm)}$, $MSI^{C}_{(mxm)}$
Verification signature image of size q×q¬$VI_{(qxq)}$ where q=n/4

Output: meaningful shares of size mxm→$MSI^{V}_{(mxm)}$, $MSI^{VC}_{(mxm)}$
Begin
Step 1: Split the images into 3 color channels.
$VI_{(q,q)}$_ { $VI_{(R)}$, $VI_{(G)}$, $VI_{(B)}$ }
$MSI^{V}_{(mxm)}$_ { $MSI^{V}_{(R)}$, $MSI^{V}_{(G)}$, $MSI^{V}_{(B)}$ }3
$MSI^{VC}_{(mxm)}$_ { $MSI^{VC}_{(R)}$, $MSI^{VC}_{(G)}$, $MSI^{VC}_{(B)}$ }
Step 2 : Do step 2-4 of algorithm 1 ? $VI_{(R)}$, $VI_{(G)}$, $VI_{(B)}$
Step 3: Dual embedding-
Repeat step 7 of algorithm 1 with i,j = q
Step 4: Repeat step 7 ? (MSI_G, MSI^{C}_{G}) and (MSI_B, MSI^{C}_{B}) using VI_G, VI_B respectively.
Step 5: Share 1 $MSI^{V}_{(mxm)}$ = cat (MSI_R, MSI_G, MSI_B)
Step 6: Share 2 $MSI^{VC}_{(mxm)}$ =cat(MSI^{C}_{R}, MSI^{C}_{g}, MSI^{C}_{B})
end

Decryption and verification: The decryption process is same as in algorithm1 except for one small difference in the displayed output. As stated earlier the shares are stacked and the secret image and the verification code is perceived by the human visual system. Method I's reconstructed output will contain the secret image in the foreground and the key used will be positioned in the center of the background. Method II's output varies only in the position of the key for in this case the key will occupy one of the four corners.

RESULTS AND DISCUSSION

Table 1, 2 and 3 show the experimental results of all the three algorithms. The parameter used to evaluate results is PSNR and ESSIM. Peak Signal to Noise Ratio (PSNR) (Ramesh Kumar and Chandramathi, 2015) represents the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation in terms of decibel (dB). PSNR is defined as:

$$PSNR = 10\lg\left(\frac{255^2}{MSE}\right)$$

The visual fidelity between two images can be predicted by the similarity between their edge-strength maps. It is called as, ESSIM (Edge strength similarity for image quality assessment) (Zhang *et al*., 2013) index and is defined as:

$$ESSIM(a,b) = \frac{1}{N}\sum i \to 1 \text{ to } N \frac{2E(a,i)E(b,i) + C}{(E(a,i))2 + (E(b,i))2 + C}$$

The parameters a and b in the above equation refer to the reference and distorted images, N is the total number of pixels in a or b, E(a, i) and E(b, i) are the edge strength at pixel "i" of images a and b respectively & C is a scaling parameter such that $C = (BL)^2$ where B is a constant and L is the dynamic range of edge strength.

PSNR and ESSIM values are calculated with reference to halftoned secret image hSI and halftone cover image hCI. We have calculated PSNR and ESSIM for three different inputs. The values of both parameters show the visual quality of the proposed methods. Also it proves that our method works for any kind of natural images with good visual quality.

Table1: Experiment results for algorithm 1

		MSI		MSIc		Reconstructed output without verification	
SI	CI	PSNR	ESSIM	PSNR	ESSIM	PSNR	ESSIM
Tiger	Baboon	54.11	1	54.14	1	52.25	0.9998
Lena	Baboon	54.11	1	54.13	1	51.13	0.9998
Normal Color Text	Baboon	54.11	1	54.16	1	48.74	0.9999

Table 2: Experiment results for algorithm 2

		MSIv		MSIvc		Reconstructed output with verification Method I	
VI	CI	PSNR	ESSIM	PSNR	ESSIM	PSNR	ESSIM
Signature	Baboon	53.13	1	53.17	1	52.25	0.9998
Text	Baboon	53.13	1	53.18	1	51.13	0.9998
Color Text	Baboon	53.13	1	53.20	1	48.74	0.9999

Table 3: Experiment results for algorithm 3

		MSIv		MSIvc		Reconstructed output with verification Method II	
VI	CI	PSNR	ESSIM	PSNR	ESSIM	PSNR	ESSIM
Signature	Baboon	54.11	1	54.14	1	52.25	0.9998
Text	Baboon	54.11	1	54.15	1	51.13	0.9998
Color Text	Baboon	54.11	1	54.16	1	48.74	0.9999

CONCLUSION

A color visual cryptography scheme for natural images was implemented which has the capability of generating meaningful shares with visually pleasing quality instead of random shares, as is found in most of the existing algorithms. Also the final stacked output of the proposed algorithm1 for natural images gives better results compared to the literature. The ESSIM value for the same is .99 which shows the visual quality. The main advantage of our verification methods is that we can verify the authenticity of the shares stacked by seeing the verification image. No additional share is needed for this process. In both the verification methods the visual quality is similar to algorithm1. This method can be used for various applications like electronic voting systems, online banking, etc.

REFERENCES

Hou, Y.C., 2003. Visual cryptography for color images. Pattern Recognit., 36: 1619-1629.

Hu, C.M. and W.G. Tzeng, 2007. Cheating prevention in visual cryptography. IEEE. Trans. Image process., 16: 36-45.

Kang, I., G.R. Arce and H.K. Lee, 2011. Color extended visual cryptography using error diffusion. IEEE. Trans. Image Process., 20: 132-145.

Nakajima, M. and Y. Yamaguchi, 2002. Extended visual cryptography for natural images. J. WSCG., 10: 303-310.

Naor, M. and A. Shamir, 1995. Visual Cryptography. In: Advances in Cryptology, De Santis, A. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-60176-0, pp: 1-12.

Naor, M. and A. Shamir, 1996. Visual Cryptography II: Improving the Contrast Via the Cover Base. In: International Workshop on Security Protocols. Mark, L. (Ed.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-540-62494-3, pp: 197-202.

Ramesh, K.R. and S. Chandramathi, 2015. Enhanced color visual cryptography using halftoning schemes. Aust. J. Basic Appl. Sci., 9: 8-14.

Verheul, E.R. and H.V. Tilborg, 1997. Constructions and properties of k out of n visual secret sharing schemes. Designs Codes Cryptogr., 11: 179-196.

Zhang, X., X. Feng, W. Wang and W. Xue, 2013. Edge strength similarity for image quality assessment. IEEE. Signal process. Lett., 20: 319-322.