Halftone Visual Cryptography for Color Images Using Error Diffusion and Direct Binary Search

Sandhya Anne Thomas and Saylee Gharge

Abstract Visual cryptography is a cryptographic technique which enhances the security of the image and uses the characteristics of human vision to decrypt encrypted images. Halftone Visual Cryptography uses halftoning techniques for converting the color image into binary images. The problem of encoding color image into *n* shares of meaningful halftone images is considered in this paper. The halftone techniques used are Error Diffusion and Direct Binary Search. Using these techniques, a secret pixel of a color image can be encoded into shares. These two techniques are compared on the basis of Peak to Signal Noise ratio (PSNR), Correlation, Universal Quality Index (UQI) and Structural Similarity (SSIM).

Keywords Visual cryptography · Halftone · Error diffusion · Direct binary search · Extended visual cryptography

1 Introduction

With the rapid development and increased need of computer and communication technology, more secret information are transmitted through the Internet. Therefore, protecting the secret information from being suspected and decrypted has become critical task. In 1994, a new information security technique called Visual Cryptography (VC) [1] was invented. VC is a cryptographic scheme in which decrypting of hidden images is done using human eyes. No previous knowledge of cryptography or computation is required for decoding which is the advantage of using in this technique along with high security offered using this technique. Visual cryptography scheme (VCS) [2] is a scheme which allows the encryption of a secret image into

S. A. Thomas (✉) · S. Gharge
Department of Electronics and Communication Engineering, VESIT, Chembur, Mumbai, MH, India
e-mail: sandhya.thomas@ves.ac.in

S. Gharge
e-mail: saylee.gharge@ves.ac.in

G. R. Kadambi et al. (eds.), *Emerging Trends in Photonics, Signal Processing and Communication Engineering*, Lecture Notes in Electrical Engineering 649,
https://doi.org/10.1007/978-981-15-3477-5_13

n shares that is given to *n* participants. These *n* participants are called the qualified shares. VC works on binary image only. Images are not only monochrome format but in grayscale and color. For converting a grayscale [3] and a color image to binary image, halftoning techniques are applied. Commonly used halftone techniques for color image encryption are Error diffusion and Direct Binary Search (DBS) which is implemented in this paper.

To explain the basic principle of VC, consider a (k, n) VC scheme which encrypts a secret image into *n* shares to be distributed among *n* participants. Each share shows a random noise pattern of black and white and doesn't disclose any information on the secret image by itself. In a (k, n) VCS, *k* is the minimum qualifying participants required to decode the secret image. Fewer participants that is *k-1* will be forbidden which will not decode the secret image even if infinite computational power is available. Qualifying share will be stacking/superimposed to decrypt the secret image. Researches have developed several methods for VC in literature. An optimal contrast *k, n* VCS was proposed to analyze the contrast of the reconstructed image for a (k, n)-threshold VCS [4]. Blundo [5] developed VCS with general structure for grayscale images. To generate a halftone share, Hou [6] transformed a gray level image into halftone images and then applied to VC. Extended visual cryptography (EVC) was developed by Ateniese [7] in which shares carry not only secret image information but meaningful images also. Meaningful images have a higher security rather than random noise shares. Hypergraphy color is used in constructing meaningful binary shares. Image quality was improved by Nakajima [8] by extended EVC with natural grayscale images. Halftone methods are used to generate good quality halftone shares in VC [9]. Meaningful Halftone image using threshold array was proposed in [10]. Meaningful images using error diffusion [11] was developed for producing halftone shares. Color Extended Visual Cryptography using error diffusion was developed by Inkoo [12] and Halftone visual cryptography using Direct Binary Search (DBS) [13].

In the above mentioned methods, the shares that are produced have low visibilities. The different types of halftoning methods are point process, neighborhood process and iterative process. Neighborhood processing (Error Diffusion) and iterative process (DBS) of halftoning are implemented and compared. Halftone is applied on both the secret images and cover images.

2 Methodolgy

Encryption In this paper, encryption for a (2, 2) VC scheme is done using EVC using halftoning techniques for color images. A secret image of size $m \times m$ is taken and halftone is applied. The methods implemented for halftoning are Error diffusion or DBS. In Error diffusion halftoning, the quantization error is distributed to the nearby pixels which are unprocessed. Also the Visual information pixels position is retained. Whereas, in DBS which is a iterative search, a binary image is taken and a template is saved. It is then processed depending on the given iterative value. Each time when the process gets completed, error is calculated and the least error found is selected as a DBS halftoned share. Share images taken for producing meaningful share of size $n \times n$ has to be double in size in comparison with the secret image. Here also halftone techniques are applied in the same manner as explained above to get two meaningful halftone shares. Encrypted share 1 and share 2 is now generated which carries both secret information and meaningful images. Now the share is ready to be given to the as qualified shares to the participant.

Decryption The qualified participant on stacking/superimposing will recover the original secret image. The stacking/superimposing is executed using the $\otimes$ the ‘OR’ boolean function.

DBS uses the minimum perceived error obtained by searching for the best possible binary value in the halftone image iterations. This gives DBS much better halftone image quality than error diffusion. This is further verified using various parameters. The parameter metrics used for analyzing the encrypted shares with the original halftoned share are PSNR, Correlation UQI and SSIM. PSNR is a measure to find of quality of recovered images and actual image. Correlation extracts the information of a image, then the encrypted share is compared with the halftoned image. UQI [14] is the ability to measure the information loss occurred during the image degradation process and SSIM [15] measures the similarity between reconstructed images and original image. By considering more parametric measures, a better understanding of the quality of the desired image can be achieved.

3 Result and Discussion

In this section, a 2-out of-2 Halftone VC is constructed using error diffusion and DBS. The secret image to be encoded is *Lena*. Two color images *Earth* and *Baboon* are taken as meaningful images. The size of the share is 256 × 256 and the size of the secret image is 128 × 128.

In Fig. 1, Fig. 1a is the original secret image which has to be encoded. Figure 1c and d are original cover images. Figure 1b, d, f are halftoned images using error diffusion. Encrypted shares generated are shown in Fig. 1g and h. Figure 1i shows the reconstructed image when encrypted shares 1 and 2 are stacked together using OR operation.

In Fig. 2, Fig. 2a is the original secret image which has to be encoded. Figure 2c and d are original cover images. Figure 2b, d, f are halftoned image using DBS. Encrypted shares generated are shown in Fig. 2g and h. Figure 2i shows the reconstructed image when encrypted shares 1 and 2 are stacked.

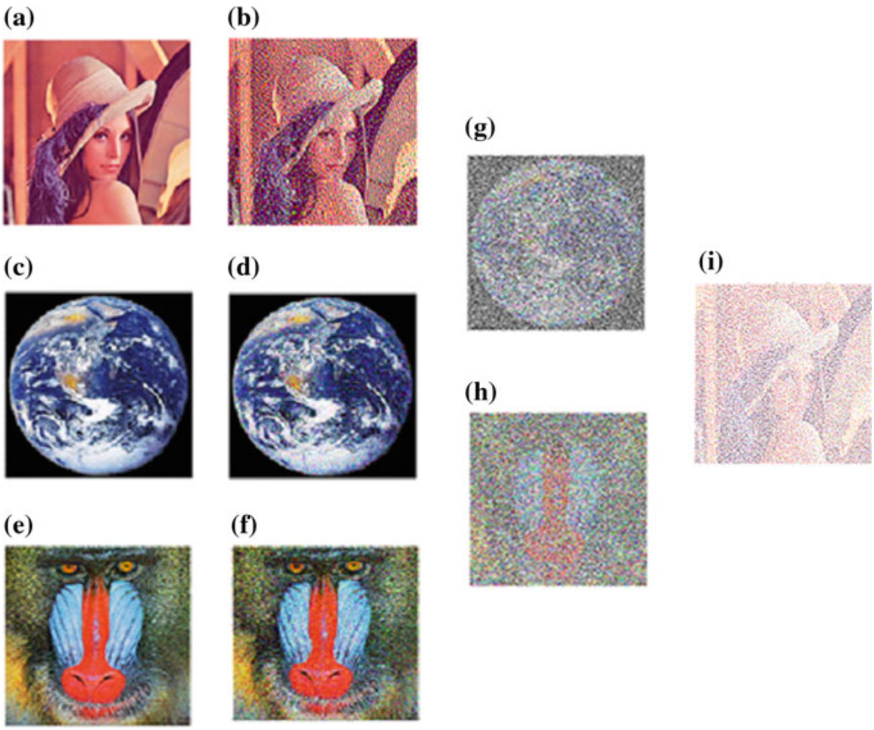

Fig. 1 Illustrative results of visual cryptography using Error Diffusion. **a** Original secret image lena, **b** halfone lena **c** and **e** original cover share image respectively, **d** halftoned earth, **f** halftoned baboon, **g** encrypted share 1, **h** encrypted share 2, **i** decrypted image

Table 1 shows PSNR, Correlation, UQI and SSIM of Encrypted Share 1 for 10 color secret images. The average value using Error Diffusion of PSNR is 51.41, Correlation is 0.3105, UQI is 0.1315 and SSIM is 0.0408. Using DBS, the average value of PSNR is 51.646, Correlation is 0.3027, UQI is 0.1331 and SSIM is 0.0843.

Table 2 shows PSNR, Correlation, UQI and SSIM of Encrypted Share 2 for 10 color secret images. The average value using Error Diffusion of PSNR is 51.291, Correlation is 0.2609, UQI is 0.0693 and SSIM is 0.0398. Using DBS, the average value of PSNR is 51.482, Correlation is 0.2788, UQI is 0.1066 and SSIM is 0.0647.

4 Conclusion

Visual Cryptography provides one of the secure ways to transfer images on the Internet. Images in color have been encoded and decoded using both Error diffusion and Direct Binary Search. Various parameters have been taken like PSNR, Correlation, UQI and SSIM. The proposed UQI model performs well without any Human Visual

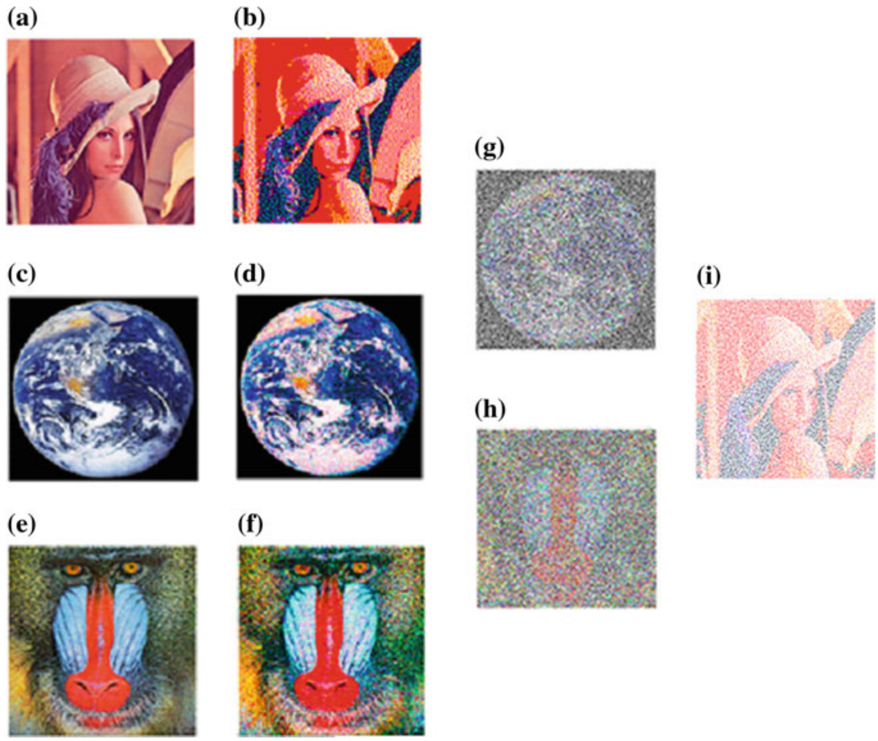

Fig. 2 Illustrative results of visual cryptography using direct binary search. **a** Original secret image lena, **b** halfoned lena **c** and **e** original cover share image respectively, **d** halftoned earth, **f** halftoned baboon, **g** encrypted share 1, **h** encrypted share 2, **i** decrypted image

Table 1 Encrypted share 1

Secret	Error diffusion				Direct binary search			
Image	PSNR	Correlation	UQI	SSIM	PSNR	Correlation	UQI	SSIM
Image text	51.411	0.3187	0.0678	0.0426	51.651	0.3066	0.1326	0.0889
Baboon	51.412	0.3188	0.6799	0.0436	51.662	0.3074	0.1350	0.0900
Barbara	51.405	0.3184	0.0665	0.0407	51.655	0.3069	0.1335	0.0883
Fruit	51.391	0.3177	0.0635	0.0382	51.653	0.3071	0.1329	0.0893
Peppers	51.417	0.3191	0.0691	0.0444	51.646	0.3062	0.1317	0.0872
Earth	51.405	0.3185	0.0665	0.0411	51.652	0.3069	0.1327	0.0880
Lena	51.368	0.2367	0.0957	0.0275	51.569	0.2642	0.1318	0.0455
Tulips	51.411	0.3188	0.0678	0.0420	51.663	0.3072	0.1350	0.0903
Vegetables	51.416	0.3190	0.0690	0.0439	51.655	0.3069	0.1334	0.0880
Space	51.416	0.3190	0.0689	0.0439	51.651	0.3070	0.1326	0.0870
Average	51.405	0.3105	0.1315	0.0408	51.646	0.3027	0.1331	0.0843

Table 2 Encrypted Share 2

Secret	Error diffusion				Direct binary search			
Image	PSNR	Correlation	UQI	SSIM	PSNR	Correlation	UQI	SSIM
Image text	51.266	0.2666	0.0615	0.0428	51.46	0.2826	0.1003	0.0696
Baboon	51.383	0.2377	0.0989	0.0264	51.586	0.2654	0.1353	0.0483
Barbara	51.393	0.2382	0.1010	0.0294	51.582	0.2652	0.1344	0.0478
Fruits	51.283	0.2676	0.0652	0.0464	51.45	0.2813	0.0983	0.0684
Peppers	51.236	0.2649	0.0551	0.0358	51.451	0.2820	0.0987	0.0678
Earth	51.286	0.2677	0.0659	0.0474	51.458	0.2824	0.0998	0.0690
Lena	51.271	0.2669	0.0627	0.0439	51.452	0.28204	0.0986	0.0677
Tulips	51.276	0.2672	0.0636	0.0444	51.467	0.2828	0.1019	0.0707
Vegetables	51.257	0.2661	0.0596	0.0412	51.437	0.2813	0.0956	0.0646
Space	51.259	0.2662	0.0599	0.0404	51.474	0.2832	0.1034	0.0730
Average	51.291	0.2609	0.0693	0.0398	51.482	0.2788	0.1066	0.06468

System model. Also algorithm supports not only monochrome images but grayscale and color images, even pixel expansion have been minimized. Correlation value is decreased in Encrypted share 1 but in the case of share 2, all the parameter measured value of DBS is better than Error Diffusion. The percentage of variation in PSNR, Correlation and UQI among these two methods is very small whereas improvement in SSIM is 50 percent in case of DBS. Visually also direct binary search gives us better results than Error Diffusion.

References

1. Naor M, Shamir A (1994) Visual cryptography. In: Proceedings of the EUROCRYPT, pp 1–12
2. Sandhya T, Saylee G (2017) Review on various cryptography schemes. In: International conference on current trends in computer, electrical, electronics and communication (ICCTCEEC), pp 360–363
3. Sandhya T, Saylee G (2018) Halftone visual cryptography for grayscale images using error diffusion and direct binary search. In: Proceedings of the 2nd international conference on trends in electronics and informatics (ICOEI) IEEE conference, pp 1091–1096
4. Blundo C, DArco P, De Santis A, Stinson DR (2003) Contrast optimal threshold visual cryptography schemes. SIAM J Discret Math 16, 224–261
5. Blundo C, Santis AD, Naor M (2000) Visual cryptography for grey level images. Inf Process Lett 75:255–259
6. Hou YC (2003) Visual cryptography for color images. Pattern Recognit 36:1619–1629
7. Ateniese G, Blundo C, Santis A, Stinson DR (2001) Extended capabilities for visual cryptography. ACM Theor Comput Sci 250:143–161
8. Nakajima M, Yamaguchi Y (2002) Extended visual cryptography for natural images. J WSCG 10
9. Zhou Z, Arce GR, Crescenzo GD (2006) Halftone visual cryptography. IEEE Trans Image Process 18:2441–2453

10. Myodo E, Sakazawa S, Takishima Y (2006) Visual cryptography based on void-and-cluster halftoning technique. In: IEEE international conference on image processing, pp 97–100
11. Wang ZM, Arce GR, Di Crescenzo G (2009) Halftone visual cryptography via error diffusion. IEEE Trans Inf Forensics Secur 4:383–396
12. Kang I, Arce GR, Lee HK (2011) Color extended visual cryptography using error diffusion. IEEE Trans Image Process 20
13. Wang ZM, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography via direct binary search. In: EUSIPCO
14. Wang Z, Bovik AC (2002) A universal image quality index. IEEE Signal Process Lett 9
15. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13