International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 12 | Dec - 2021 ISSN: 2582-3930

Image Encryption: Investigation towards Halftone Visual Cryptography

Sunesh

IT Department, MSIT, New Delhi

Abstract - The digital revolution era uplifts the generation, storage and sharing of digital content over the internet. Visual Cryptography is one of the image encryption methods in order to ensure security of images. Visual cryptography encodes image into distinct shares. This paper presents a study on HVC with error diffusion method. The halftone visual cryptography scheme utilizes the error diffusion halftoning and visual secret sharing principles to generate the halftone shares

Key Words: Image encryption, HVC, Error diffusion based HVC , Security, image

1. INTRODUCTION

The fast storage and transmission of digital images demands the way to deal with security concern with less computing and fast processing. In the field of image encryption, Visual cryptography is one of most promising technology, first anticipated in 1994 by Naor and Shamir [1]. The concept of visual cryptography encodes image into image shares in a manner that it can decoded by human vision only if right key is used.[9] It is very difficult to extract any information from the encoded share[6]. The visual cryptography schemes majorly divided into two categories. One is (2, 2) VC and second is (k,n) VC. The (2, 2) Visual cryptography scheme encodes the image and generates the two distinct shares and decoding process requires both shares to get the original image. Whereas, the (k,n) visual cryptography scheme encodes images into n distinct shares and minimum k shares are require obtain the original image.

The present paper investigates (2,2) Halftone visual cryptographic Scheme using image size invariant technique. The halftone visual cryptography method may classify into distinct ways based on the method like error diffusion, Classical screening, dithering, direct binary search. In this paper, HVC with error diffusion method has been studied.

This paper is organized into four distinct sections. Section 2 presents the related work and section 3 presents the halftone visual cryptography process. Performance of HVC will be discussed. Lastly, Section 5 concludes the paper.

2. RELATED WORK

In the field of visual cryptography, a lot of work has been reported in the literature. The journey of visual cryptography is depicted through Figure1. The visual cryptography techniques like color image VC, probabilistic VC, extended VC, halftone VC has been illustrated in figure1[1-4,7,]. In history, different halftone visual cryptography scheme like HVC based on error diffusion, Classical screening, dithering, direct binary search has been developed by the researchers[8,10-11, 14,16]. (2,2) HVC, (k,n) HVC, size invariant HVC were also proposed in literature. Halftone Visual Cryptography uses the halftone image as input which is very small is size hence requires small memory space[2,16,11]. The encryption process is very secure because the noise generation is random and it doesn't given any information about the secret information[2,5]. HVC is very robust and retains the original quality of the encrypted image after decryption.

The present paper discusses size invariant (2,2) halftone visual cryptography method. The concept of error diffusion was given by Floyd and Steinberg in 1976[13]. The error diffusion has better features than the classical screening method. The error diffusion utilizes the neighborhood procedure and threshold. Error diffusion method is one of vital method in halftoning method.

Expedition of visual cryptography	
	Fundamental visual cryptography by Naor and Shamir
	Investigation on distinct issues like contrast, pixel expansion and distinct formats
	Threshold VC with perfect black pixel reconstruction
	General VC access structure
	Color Image visual cryptography
	Multiple secret sharing
	Threshold VC with distinct whiteness level
	To improve visual quality of VC
	Probabilistic VC with different thresholds
	Generalization of Probabilistic VC
	Extended visual cryptography
	Extended visual cryptography with range distribution
	Halftone visual cryptography
	Halftone visual cryptography with error diffusion

Figure 1: Journey of visual cryptography

3. Halftone Visual Cryptography Process

The halftone visual cryptography HVC utilizes the halftoning concept to accomplish the encryption. The basic process of (2,2) HVC method is explained in Figure 1. The halftone visual cryptography process includes halftoning, share encryption and share decryption.

The process of halftoning simulates the tones of gray by different the size of dots organized in the regular pattern. Halftoning by Error Diffusion refer to the diffusing of quantization error along the path of image scan. Generally, the error diffusion halftoning involves thresholding, error computation, error distribution to neighbhor. Diffusing error to pixels has 3 different types namely Jarvis algorithm, stuki algorithmand Floyd Steinberg algorithm.

Share encryption encrypts the original image into shares. The basic matrix in Visual cryptography is utilized with halftone visual cryptography to encrypt every pixel into 2 different pixels in 2 different shares but at the same position.

The share decryption decrypts the share and generates the original image. In the decryption, bitwise XOR operation is performed to retrieve the original image. The retrieved image look likes the original image.

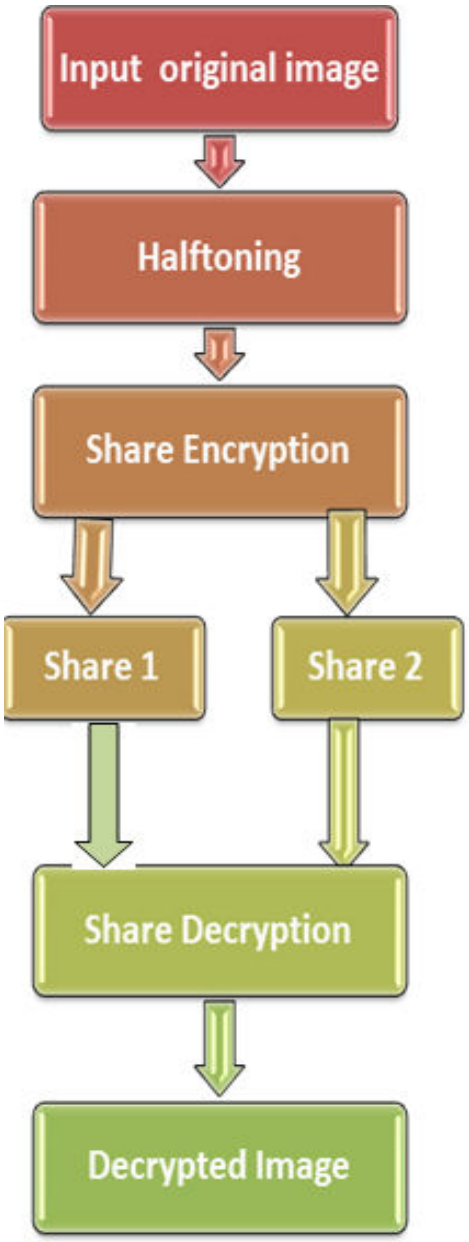

Figure2: Basic HVC Process

4. Discussions

The performance of halftone visual cryptography is measured through PSNR, MD, SC and many more. All quality metrics admit the changes to the noise powers variation. MD appears to be the most sensitive metric whereas SC being the least sensitive to the difference in noise power. From figure3 and figure 4, it is clear that SSIM give results with greater accuracy. In this section, HVC results under distinct attacks like Gaussian and salt and noise attack has been discussed.

Initially, The behavior of halftone visual cryptography under Gaussian noise attack has been presented in the given below Figure 3.

Secret Image	Image Size	Pre-Attack PSNR			Post-Attack PSNR		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	Inf	3.0053	2.7894	54.1854	3.324	3.1119
Barbara	512x512	Inf	2.9966	2.7945	54.1854	3.309	3.1112
Baboon	512x512	Inf	3.0132	2.7832	54.1854	3.3281	3.1028
Goldhill	512x512	Inf	2.9818	2.7928	54.1854	3.296	3.1086
Elaine	1024x1024	Inf	3.0262	2.7893	60.206	3.3402	3.1059

Secret Image	Image Size	Pre-Attack SC			Post-Attack SC		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	1	0.0045	-0.044	1	0.0021	-0.042
Barbara	512x512	1	2.8e4-04	-0.037	1	0.0021	-0.040
Baboon	512x512	1	0.0014	-0.044	1	0.0017	-0.047
Goldhill	512x512	1	-6.9e-04	-0.040	1	0.0022	-0.039
Elaine	1024x1024	1	0.001	-0.043	1	0.0014	-0.043

Secret Image	Image Size	Pre-Attack MD			Post-Attack MD		
		Secret Image	Share 1	Share 2	Secret Image	Share 1	Share 2
Lena	512x512	0	1	1	0	1	1
Barbara	512x512	0	1	1	0	1	1
Baboon	512x512	0	1	1	0	1	1
Goldhill	512x512	0	1	1	0	1	1
Elaine	1024x1024	0	1	1	0	1	1

Secret Image	Image Size	Pre-Attack NAE			Post-Attack NAE		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	0	1.0301	1.089	0	1.0326	1.0849
Barbara	512x512	0	1.0937	1.1408	0	1.0915	1.1436
Baboon	512x512	0	0.9836	1.0339	0	0.9826	1.036
Goldhill	512x512	0	1.1474	1.1962	0	1.1442	1.1966
Elaine	1024x1024	0	0.9326	0.9842	0	0.9325	0.9836

Figure 3: HVC results under Gaussian attack

The performance of size invariant HVC also studied in Salt and Pepper attacked environment. In this , Salt and Pepper noise is added to one of the shares and then decrypted it. The results are depicted in the Figure 4.

Secret Image	Image Size	Pre-Attack PSNR			Post-Attack PSNR		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	Inf	3.0053	2.7894	13.1607	2.9984	2.7886
Barbara	512x512	Inf	2.9966	2.7945	13.1535	3.002	2.7973
Baboon	512x512	Inf	3.0132	2.7832	13.0677	3.0096	2.7917
Goldhill	512x512	Inf	2.9818	2.7928	13.1086	2.9746	2.8072
Elaine	1024x1024	Inf	3.0262	2.7893	13.0994	3.0197	2.7994

Secret Image	Image Size	Pre-Attack SC			Post-Attack SC		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	1	0.0045	-0.044	0.8856	0.0018	-0.039
Barbara	512x512	1	2.8e4-04	-0.037	0.8778	-0.036	-0.002
Baboon	512x512	1	0.0014	-0.044	0.8941	0.0025	-0.045
Goldhill	512x512	1	-6.9e-04	-0.040	0.8756	0.0014	-0.038
Elaine	1024x1024	1	0.001	-0.043	0.8851	0.0017	-0.041

Secret Image	Image Size	Pre-Attack MD			Post-Attack MD		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	0	1	1	1	1	
Barbara	512x512	0	1	1	1	1	1
Baboon	512x512	0	1	1	1	1	1
Goldhill	512x512	0	1	1	1	1	1
Elaine	1024x1024	0	1	1	1	1	1

Secret Image	Image Size	Pre-Attack NAE			Post-Attack NAE		
		Secret Image	Share1	Share2	Secret Image	Share1	Share2
Lena	512x512	0	1.0301	1.089	0.1006	1.0337	1.0824
Barbara	512x512	0	1.0937	1.1408	0.1056	1.0961	1.1381
Baboon	512x512	0	0.9836	1.0339	0.0957	0.9821	1.0344
Goldhill	512x512	0	1.1474	1.1962	0.1128	1.1452	1.1938
Elaine	1024x1024	0	0.9326	0.9842	0.0916	0.9322	0.9816

Figure 4: HVC results under Salt and pepper attack

5. Conclusion

Halftone Visual Cryptography in the market is very promising technology. It enables the secret sharing of grayscale images and even color images. The technique of Halftone Visual Cryptography has been successfully carried out. In this paper, size invariant secret sharing scheme has been discussed in which image halftoned and visual secret is sharing algorithm is applied on it. The halftone visual cryptographic technique may be applied to the existing area in which uses the visual cryptography and demands high image quality. The presented scheme is not much immune to rotation, blurring attacks on shares which are transmitted but it retains the image quality in noise, cropping and lossy compression attack or the information to some extent.

REFERNCES

[1] Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in Cryptology—EUROCRYPT'94. Springer Berlin/Heidelberg, 1995.
[2] Zhou, Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." IEEE transactions on image processing 15.8 (2006): 2441-2453.
[3] Chen, Qin, et al. "An extended color visual cryptography scheme with multiple secrets hidden." Computational and Information Sciences (ICCIS), 2010 International Conference on. IEEE, 2010.
[4] J. P. Weir and Weiqi Yan, "Visual Cryptography and Its Applications", Bookboon, 2012
[5] Alkharobi, Talal Mousa, and Aleem Khalid Alvi. "New Algorithm for Halftone Image Visual Cryptography." IEEE 2004 (2004).
[6] Shankar, K., and P. Eswaran. "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography." Procedia Computer Science 70 (2015): 462-468.
[7] Chandramathi, S., et al. "An overview of visual cryptography." International Journal of Computational Intelligence Techniques, ISSN (2010): 0976-0466.
[8] Wang, Zhongmin, and Gonzalo R. Arce. "Halftone visual cryptography by iterative halftoning." Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on. IEEE, 2010.
[9] Dang, Wanli, et al. "K out of K Extended Visual Cryptography Scheme Based on" XOR"." International Journal of Computer and Communication Engineering 4.6 (2015): 439.
[10] Kamboj, Aman, and D. K. Gupta. "An improved Halftone Visual Secret Sharing Scheme for gray-level images based on error diffusion in forward and backward direction." Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on. IEEE, 2015.
[11] Chaturvedi, Amit, and Imtiyaz Rehman. "Analysis of the HalfTone Visual Cryptography and proposing a model for illustrating the related schemes."
[12] Pujari, Vandana G., Shivchandra R. Khot, and Kishor T. Mane. "Enhanced visual cryptography scheme for secret image retrieval using average filter." Wireless Computing and Networking (GCWCN), 2014 IEEE Global Conference on. IEEE, 2014
[13] Ostromoukhov, Victor. "A simple and efficient error-diffusion algorithm." Proceedings of the 28th annual conference on Computer graphics and interactive techniques. ACM, 2001.
[14] N. H. M. H. a. C. R. M. Askari, "An extended visual cryptography scheme without pixel expansion for halftone images," p. 6, 2013.
[15] Z. G. R. A. a. G. D. C. Zhou, "Halftone Visual Cryptography," "Halftone visual cryptography" IEEE transactions on image processing 15.8 (2006): 2441-2453, vol. 15.8, 2006.
[16] A. a. I. R. Chaturvedi, "A Review of Halftone Visual Cryptography Schemes," vol. 5.12, 2015.