Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.134 – 140

RESEARCH ARTICLE

Comparative Analysis on Visual Cryptographic Schemes

T. Anuradha[1], K. Usha Rani[2]

[1]Research Scholar, Department of CS, Sri Padmavathi Mahila Viswavidyalayam, Tirupati, India

[2]Professor, Department of CS, Sri Padmavathi Mahila Viswavidyalayam, Tirupati, India

[1] a_talasila@yahoo.com; [2] usharanikiruba@yahoo.co.in

Abstract— Visual cryptography is the techniques that deal with providing security to the multimedia data. The main concept behind this is, to encrypt a secret image into some shares. The secret can be revealed only when all the shares are combined. The central theme of visual cryptography is that it doesn't require any manipulation or tough cryptographic knowledge and the decryption is done by human vision without the help of computers. Thus, visual cryptography is known for its least computational complexity yet much secure. In this work, we compared traditional visual cryptography, extended visual cryptography and colour extended cryptography with respect to PSNR, NCC and MSE. On analysis, it is found that the performance of colour extended visual cryptography is much better than the traditional visual cryptography and extended visual cryptography, in terms of Peak Signal to Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC) and Mean Square Error (MSE).

Keywords— Visual Cryptography, Extended Visual Cryptography, colour extended visual cryptography, PSNR, NCC, MSE

I. INTRODUCTION

The present era can be called as an era of data, as everyone deals with the multimedia data. Obviously, the multimedia data is transferred through the networks, which are prone to several security breaches. Proper care has to be rendered while transferring important secret images, as the adversaries may hack the data. Visual cryptography is the techniques that deal with providing security to the multimedia data.

Visual Cryptography is a technique used to protect image based secrets. The main concept behind this is, to encrypt a secret image into some shares. The secret can be revealed only when all the shares are combined. Thus, this scheme is very effective. Visual cryptography hides secrets within images. These images are encoded into multiple shares and decoded afterwards without any computation.

Visual cryptography is an emergent cryptographic methodology, which is proposed by Naor and Shamir [1]. The central theme of visual cryptography is that it doesn't require any manipulation or tough cryptographic knowledge and the decryption is done by human vision without the help of computers. Thus, visual cryptography is known for its least computational complexity yet much secure [2].

Visual cryptography safeguards image based secrets. In this scheme, a secret image is encrypted into certain shares. The secret image can be made known, only when all the shares are available, i.e. a secret image cannot be identified with some shares. The secret image can be accessed after stacking all the shares. In this paper, a survey about visual cryptography is presented.

The most useful type of visual cryptography is Colour visual cryptography. The main reason behind this is that the usage of colour images is more and also, natural coloured images are the best covers to hide a secret without any suspicions. The main application of visual cryptography is watermarking.

II. DIFFERENT VC SCHEMES

A. Traditional Visual Cryptography

Visual cryptography is proposed in [1] and defined as a new type of cryptographic scheme, which can decode concealed images without any cryptographic computation [3]. Thus, the decryption depends on the human visual system. When k number shares are stacked, human eyes decrypt. Thus, this methodology is simple yet secure.

This traditional visual cryptography claims the encryption as k out n secret sharing problem. Some of the necessary parameters of this system arem, α, γ. Here, m is the total number of pixels in a share, which can indicate the loss of resolution, α indicates the contrast loss and finally γ represents the size of C_0 and C_1, where C_0 is the sub-pixel pattern of white pixel share and C_1 is the sub-pixel pattern of black pixel share. In (2,2) Visual Cryptographic System (VCS), the shares are framed by

$$C_0 = Permute\ the\ columns\ of \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad (1)$$

$$C_1 = Permute\ the\ columns\ of \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad (2)$$

From (1) and (2), a pixel from the original image is expanded to four pixels and the shares are generated.

For a white coloured pixel in the original image, the same pattern of four pixels is randomly chosen for both the shares and for a black coloured pixel, complementary pair pattern is chosen, thus the patterns from the same column. The shares can be vertical, horizontal or diagonal.

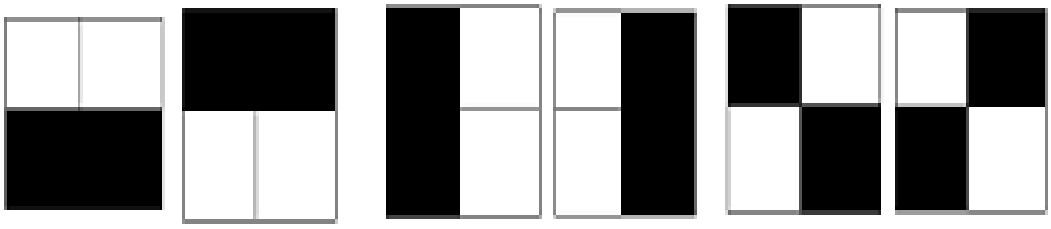
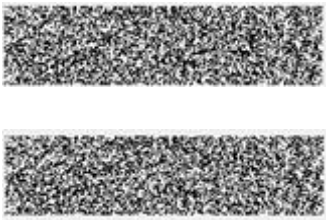


Fig 1: (a) (b) (c)

Fig 1: (a) Horizontal shares (b) Vertical Shares (c) Diagonal Shares

The main merit of this scheme is individual share cannot infer any information and thus no decryption is made possible. Many enhancements have been proposed by keeping this concept as base [4]. In [5], the concept of pixel expansion as described earlier is eliminated and it uses the (k, n) scheme. Size invariant shares are handled by a probabilistic approach [6]. In this system, the sizes of the original images and shadows remain the same. The recursive visual cryptography considers two shares which contains more than a secret. The process of secret recovery is done by applying rotation or shifting the share to various spots over the share.

TABLE I
TRADITIONAL VISUAL CRYPTOGRAPHY

Key Image	Shares	Extracted Key Image
Ph.D CS		

Traditional visual cryptography employs black and white coloured pixels to represent a binary image. Thus, it withstands the image altering attacks such as scaling, resizing, cropping, skewing etc., This is because,

the black pixel is black at all times and so is white pixel and there is no intermediate point. Thus, the security of this scheme is appreciable. However in this digital image world, the usage of binary images is vanished.

B. Extended Visual Cryptography

In traditional cryptographic systems, shares are created as random patterns of pixel, which resembles the noise. This may alert the hackers for analysis. Extended visual cryptography is proposed in [7].

Extended visual cryptography extends the nature of traditional visual cryptography but the shares are meaningful. When the shares are laid one above the other, the meaning gets disappeared and the secret is recovered. The shares must be meaningful which can be like a cat, a vehicle or something meaningful. The pixels can either be black or white. There are three conditions that must be satisfied while encrypting images. Secret image must be made known upon superimposing by the image that belongs to access structure. On analysing the shares, it must not be possible to sniff a clue about the secret. The image within the shares should not be modified by any means. A (k, n) problem is addressed in [8] and the pixel expansion is carried out in a better way than traditional visual cryptography.

TABLE III
EXTENDED VISUAL CRYPTOGRAPHY (EVC)

Key Images	Shares	Extracted Key Image
 	 	 

A work on improving the share quality in extended visual cryptography is proposed in [9]. This is attained by employing grey pixels rather than black and white pixels. In [10], uses halftone greyscale images as the medium of visual information based on EVC. Traditional visual cryptography involves several random patterns of dots, which alerts the hackers. On the other hand, when halftone shares are employed then it is quite difficult to detect encryption. This improves the security. In [11], the quality of the shares is improved by contrast enhancement techniques but they are not secure.

C. Color Visual Cryptography

Colour visual cryptography is the most useful methodology because every man in this world started to use colour images and thus natural coloured images can be used for secret sharing. Colour images are very famous and are used by most of the people. Most of the techniques use halftoning with colour visual cryptography.

In [12], two opaque and a transparent colours are used. The main thing here is to mind the order of the shares. Thus, every share is needed to be pre-determined. There are two means of constructions. They are monochromatic and bi-chromatic methodologies.

In monochromatic construction, every pixel in the original image is mapped with n number of subpixels and each participant has n sheets.

In [13], a scheme based on halftoning with colour image sharing is proposed. Halftoning technique can have different degrees of grey colours. Also, there is no need of computers to decrypt. Another system with eight colours based on RGB-CMYK colour model is proposed in [14]. In this work, all the colours are permuted when two shares are produced. The original image is generated after superimposition of shares.

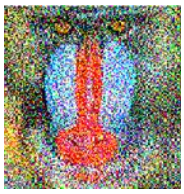
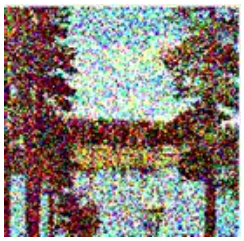
In [15], it is proven that the colour-optimal schemes are applicable for colour visual cryptography schemes. In [16], a probability based additive colour mixing scheme is proposed. This system works for a fixed pixel expansion and is an improvement over existing colour secret sharing schemes. The main drawback of the system is that the overall contrast is reduced after the secrets are revealed.

TABLE IIIII
(1,1) CEVC

Color Image	Share by error diffusion	Key Image	After Embedding	Extracted Image
				

Mostly, the colour image is darkened when the shares are laid one over the other for secret recovery. This is because, when the same coloured pixel meets each other, the resultant pixel gets darkened. This colour darkening issue is solved in [17] by concentrating only on three colours for superimposition and they are black, white and a pixel of the provided colour, which in turn yields perfect image reconstruction.

TABLE IVV
(2,2) CEVC

Color Image 1 & 2	Share by error diffusion	Key Image	After Embedding	Extracted Image
 	 		 	

III. PERFORMANCE ANALYSIS

In this work, we compared traditional Visual Cryptography (VC), Extended Visual Cryptography (EVC) and Colour Extended Visual Cryptography (CEVC) by PSNR, MSE and NCC by using Matlab as simulator. On analysis, it is found that the performance of CEVC is much better than the traditional visual cryptography and extended visual cryptography and is proved by PSNR ratio, normalized correlation coefficient and MSE. The results of analysis are presented in Table V.

A. Peak Signal to Noise Ratio(PSNR)

This performance metric evaluates the image quality between original and the cryptographic image and is calculated by (3).

$$PSNR = 10 \times log_{10} \frac{255 \times 255}{\frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2} \quad (3)$$

where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and cryptography image, respectively.

B. Normalized Correlation Coefficient (NCC)

This metric measures the quality of key image. The quality of extracted and the original key image is evaluated by (4).

$$NCC = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{i=1}^{N} E(x,y) \times O(x,y) \quad (4)$$

where M and N are the height and width of the image and E(x,y) and O(x,y) are the grey levels located at coordinate (x,y) of the extracted key image and original key image, respectively.

C. Mean Square Error (MSE)

This metric represents the cumulative squared error between the original and cryptographic image. The lower the MSE, the higher the accuracy rate and is calculated by (5).

$$MSE = \frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2 \quad (5)$$

where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and cryptography image, respectively.

TABLE V
PERFORMANCE ANALYSIS

Image	**PSNR Analysis**			**NCC Analysis**			**MSE Analysis**		
	VC	**EVC**	**CEVC**	**VC**	**EVC**	**CEVC**	**VC**	**EVC**	**CEVC**
Lena	13.321	18.215	25.427	1	1	1	17.8214	12.4531	5.6442
Boat	14.272	19.732	26.285	1	1	1	16.7421	11.3284	4.2135
Pepper	16.274	21.296	28.146	1	1	1	17.1547	12.1346	5.1456
Sail Boat	11.263	16.319	23.167	1	1	1	16.7317	11.3185	4.2361
Barbara	14.126	19.615	26.154	1	1	1	17.1536	12.1267	5.1462

Corresponding graph for Table V is provided in figures 2-4. The PSNR analysis is presented in Fig 2. Fig 3 and Fig 4 depicts NCC and MSE analysis respectively.

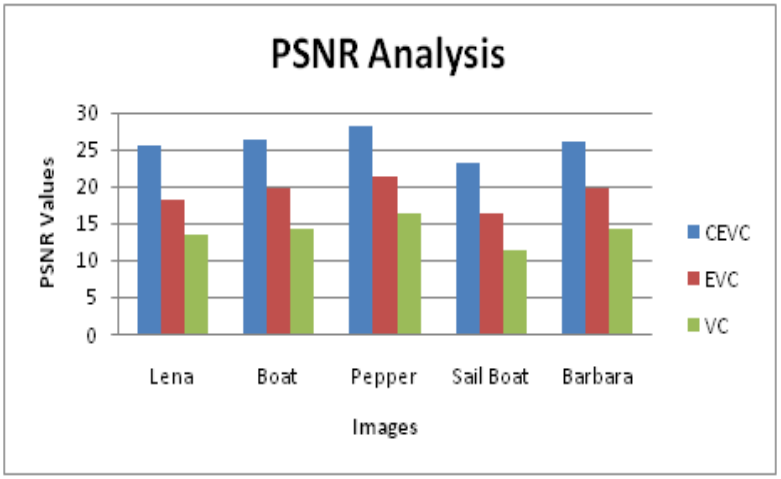


Fig 2: PSNR Analysis

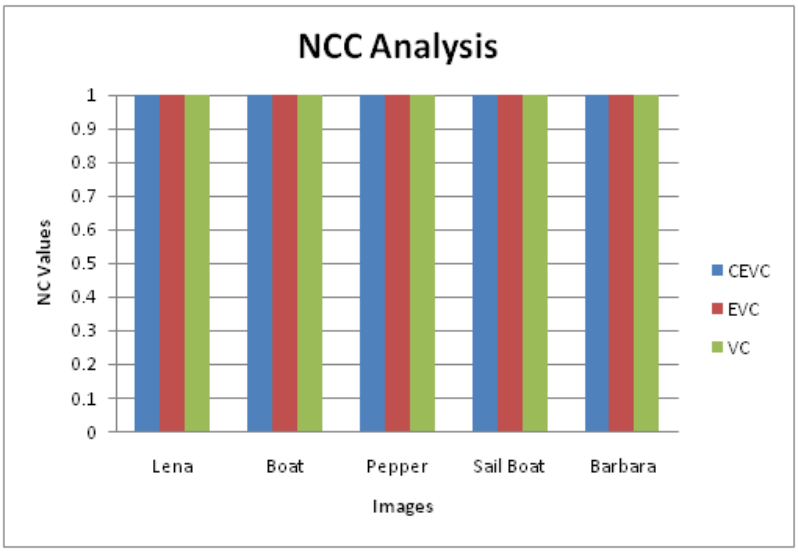


Fig 3: NCC Analysis

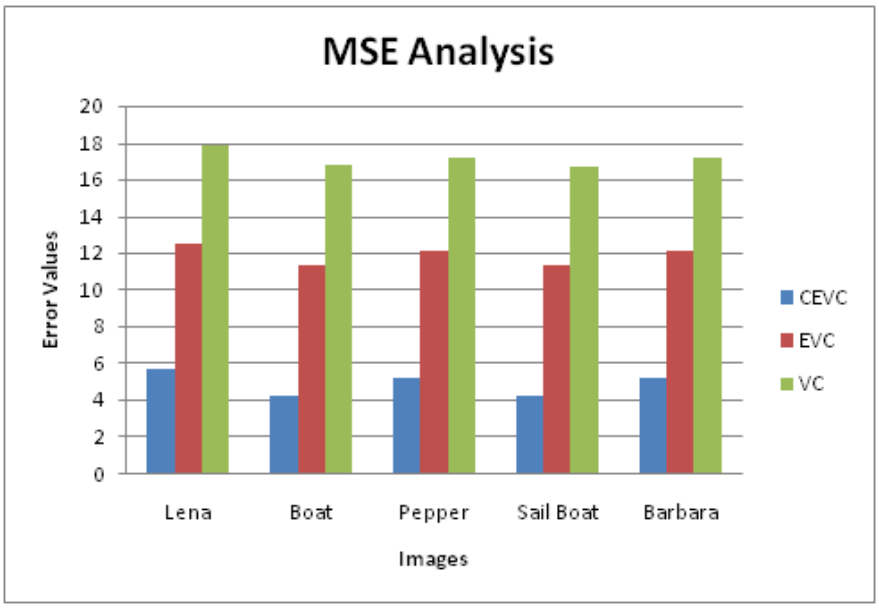


Fig 4: MSE Analysis

From the graphs, it is evident that the CEVC outperforms VC and EVC. The PSNR value for CEVC is the greatest and MSE value of CEVC is the least when compared to VC and EVC.

IV. CONCLUSIONS

In this work, the performance of traditional visual cryptography, extended visual cryptography and colour extended cryptography are evaluated. The results obtained from colour extended cryptography is satisfactory than the other two. CEVC gains the maximum PSNR value and the least MSE value. Thus in future, we propose to exploit colour extended visual cryptography.

REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, pp 1-12,1995.
[2] P.S.Revenkar, Anisa Anjum, W.Z.Gandhare, "Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications, Vol. 4, pp.49-56, 2010.
[3] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt '94, Vol 950, pp 1-12,1994.
[4] Wen-Guey Tzeng and Chi-Ming Hu, "A new approach for visual cryptography", Designs, Codes and Cryptography, Vol.27, pp.207-227, 2002.
[5] Ryo Ito, Hidenoir Kuwakado and Hatsukazu Tanaka, "Image size invariant visual cryptography", IEICE Transactions, Vol.10, pp.2172-2177, 1999.

[6] Ching-Nung Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognition Letters, Vol.25, pp.481-494, 2004.
[7] Nakajima M. and Yamaguchi Y, "Extended visual cryptography for natural images", Journal of WSCG, Vol 10, pp.303-310, 2002.
[8] Marcelo Bertalmio, Guillermo Sapiro, Vincent Caselles and Coloma Ballester, "Image inpainting", SIGGRAPH '00: Proceedings of the 27th annual conference on computer graphics and interactive techniques, New York, pp.417-424, 2000.
[9] Ching-Nung Yang and Tsse-Shih Chen, "Extended visual secret sharing schemes with high quality shadow images using grey subpixels", Lecture Notes in Computer Science, Vol.3656, pp.1184-1191, 2005.
[10] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, Vol 15, pp. 2441-2453, 2006.
[11] Mizuho Nakajima and Yasushi Yamaguchi, "Extended Visual Cryptography for Natural Images", In WSCG, pp.303-310, 2002.
[12] Moni Naor and Adi Shamir, "Visual Cryptography II: Improving the contrast via the cover base", Proceedings of the International Workshop on Security Protocols, London, pp: 197-202, 1997.
[13] Y. C. How, C. Y. Chang and S. F. Tu, "Visual cryptography for color images based on halftone technology", Image, Acoustic, Speech and Signal Processing, Part 2, 2001.
[14] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and grey-scale images", IEICE Transactions Fundamentals, Vol. 81, pp. 1262-1269, 1998.
[15] Hao Luo, Jeng-Shyang Pan and Zhe-Ming Lu, "Hiding multiple watermarks in transparencies of visual cryptography", Intelligent Information Hiding and Multimedia Signal Processing, Vol.1, pp.303-306, 2007.
[16] Ching-Nung Yang and Tse-Shih Chen, "Colored visual cryptography scheme based on additive color mixing", Pattern Recognition, Vol.41, pp.3114-3129, 2008.
[17] Shou Liu, Xiangsu Zhang and Hingkai Lai, "Artistic effect and application of moiree patterns in security holograms", Applied Optics, Vol.34, pp. 4700-4702, 1995.

