International Journal of Soft Computing 10 (2): 175-182, 2015
ISSN: 1816-9503

A New Semantic Visual Cryptographic Protocol (SVCP) for Securing Multimedia Communications

[1]A. John Blesswin, [1]P. Visalakshi, [2]M. Karnan and [3]R. Sivakumar
[1]Department of Electronics and Communication Engineering,
PSG College of Technology, 641004 Coimbatore, India
[2]Department of Computer Science and Engineering,
[3]Department of IT, Tamilnadu College of Engineering, 641659 Coimbatore, India

Abstract: Multimedia Files (MFs) are widely used in communications which has large data volume of video and audio equipped with cell phones, laptops, cameras and other devices that using multimedia contents. It is highly challenging to provide security for multimedia communication. The traditional cryptography framework encrypts the entire multimedia file which was more complex, time-consuming and tedious process. Visual Cryptography (VC) is an innovative encryption technique used in the secure transfer of images and solves the problems of computational complexity. The study considers the problem of encoding a secret image into n shares of meaningful images. Researchers propose a new Semantic Visual Cryptographic Protocol (SVCP) that can encode the secret images into the shares using error reduction and LSB embedding procedure. The noises introduced by encoded secret pixels are totally reduced and will obtain the pleasing shares. The implementation part begins with converting a grayscale image into a semantic image through error reduction followed by embedding semantic image into n shares. Finally, secret image will reconstruct without showing any interference with the share images. The experimental result shows the effectiveness and advantages of the proposed SVCP and it ensures the security and quality of the reconstructed secret images.

Key words: Communication, Visual Cryptography (VC), complex, meaningful image, error reduction

INTRODUCTION

Information Security (IS) has become one of the key focus areas of Large Scale Multimedia Communications (LSMC). In the world, Information Security (IS) faces a new challenge every day. The success of the internet is the ability to share information instantly. At the same time, various confidential data such as military maps, space images taken using satellite and commercial identifications are transmitted over the internet. Figure 1 shows the number of image security applications that encode secret information in electronic media as of 2008 (Fridrich, 2009). Visual Cryptography is one of the ways to share the visual secret information securely. The share images contain the patterns of black and white pixel combinations. For the effective management of visual cryptography, many schemes are developed by the researchers. The study proposes Semantic Visual Cryptographic Protocol (SVCP) for sharing the secret grayscale images. Secret image pixels are embedded into shares. The share images are resulted based on the cover images. For encoding the visual information, the error

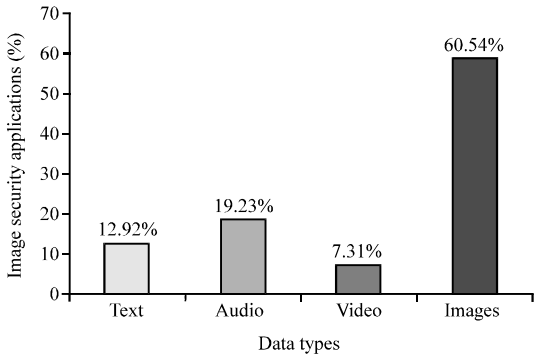

Fig. 1: The number of applications that encode the secret information in electronic media

reduction approach is proposed. In this research, SVCP is presented for grayscale images with no pixel expansion which represent the resultant image in the same size as the original secret image. Visual Secret Sharing (VSS) schemes are used in many applications like secure online money transfer, server authentication, remote voting, transmission of financial information, banking

Corresponding Author: A. John Blesswin, Department of Electronics and Communication Engineering,
PSG College of Technology, 641004 Coimbatore, India

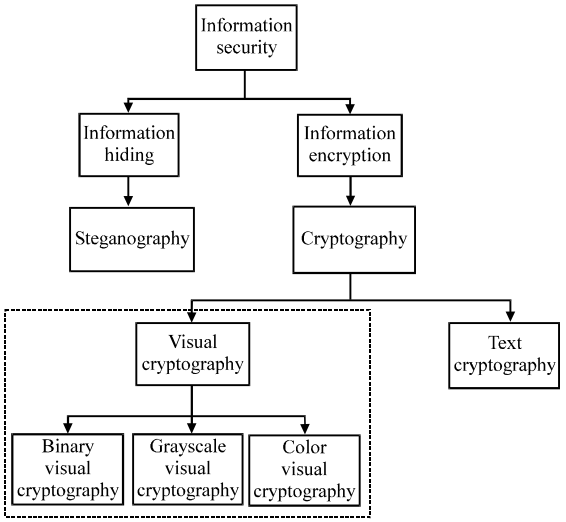

Fig. 2: The security systems disciplines. The dashed shape indicates the scope of this study

applications, medical applications and secure transfer of images over the internet, etc. A visual cryptography scheme can be mathematically defined as follows the main processes are graphically represented in Fig. 2.

Over the last few decades, multimedia information is widely used for communications and it is capable of holding more memory spaces than text files. For example, to encrypt a small image by using traditional cryptography method, it is a very tedious process because it takes more number of computational calculations and a time-consuming problem. So, there is a great need for a simple method to send visual information securely and that innovative method must meet the following goals. First, the VC Method is easy to encode the secret message with less computational calculations. Secondly, it must not a time-consuming process. Lastly, encrypted information must secure and reconstructed image have been in good quality. Naor and Shamir (1994) proposed the Visual Cryptography Scheme (VCS) which satisfied the above goals. It helps to share the secret binary information, in the most productive way.

To describe the principles of Visual Secret Sharing (VSS), consider a model of Naor and Shamir (1994) scheme as shown in Table 1. The idea of their scheme is to generate two share images by the combinations of black and white pixels according to the secret image. Ateniese *et al.* (1996) designed a novel technique to bring k out of n visual cryptography schemes. It is unable to get any secret information by stacking a less number of favorable shares. Wu (1998) invented a scheme to share more than one secret image in two random shadows. Ito *et al.* (1999) minimized the size of share images by

Table 1: Model of Naor and Shamir (1994) scheme

Images	White pixel	Black pixel
Share 1		
Share 2		
Share 1 x Share 2		

invariant visual secret sharing scheme. To encode a secret image into the same pixel dimension the shares. The above visual cryptography schemes for binary images (Naor and Shamir, 1994; Ateniese *et al.*, 1996; Wu, 1998; Ito *et al.*, 1999) which applied to carry out the work of generating shares with higher efficiency and less detecting ability.

Wang *et al.* (2006) came out with an idea of searching better option to find the configuration of binary values in the halftone images which resulted in better quality of reconstructed images. Self verifying Visual Secret Sharing Method (Chang *et al.*, 2009) helps to verify the reliability of the secret image by halftone logos. Wang *et al.* (2009) applied the technique of error diffusion to do the halftone operation on secret images. Derive the error values and distributed to their adjacent pixels which increases the reconstructed image clarity. Embed the random share into cover images which provides high security of the reconstructed secret image as offered by Liu and Wu (2011). To overcome the pixel expansion problem of Liu and Wu (2011) Model, Lee and Chiu (2012) modified the scheme into general access structures with covering images to each shadows. Askari *et al.* (2013) proposed the extended visual cryptography scheme which is used to select the cover image for embedding the share images thereby providing opportunities for integrating visual secret sharing scheme and biometric security techniques. Babu *et al.* (2013) proposed information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security. Share images are generated by bit level decomposition approach having capability of sharing a secret image which was defined by Lukac and Plataniotis (2005). To optimize the performance of pixel expansion, Fang and Yu (2006) suggested a (2, n) scheme based on minimal pixel combinations. Nakajima and Yamaguchi (2002) suggested the way of making meaningful binary images as shadows in extended visual cryptography for natural images. A segment based VC approach introduced by Borchert (2007), takes secret information, encoded in the form of segments. By seeing all the above VCS, a robust visual cryptography protocol is preferred to be employed for grayscale images which offers better imperceptibility without compromising quality and security by adapting LSB embedding procedure.

Error reduction: The following Error Reduction (ER) technique transforms a grayscale image GI into semantic image SI. The simple and attractive idea of this technique is reduction of errors thus meaning of the image is not lost. The semantic image will generate, based on a semantic error filter strategy.

The noise introduced by the encoded secret pixel can reduce which helps to reconstruct the secret image clearly without showing any interference with the help of shares. A flowchart of error reduction is shown in Fig. 3. In this study, researchers describe the new semantic error filter strategy, named SEF which helps to get the coefficients in integer form. The semantic image SI can generate based on an error reduction strategy also called an error filter. The SEF has a set of kernel weights. A signal consisting of present error value passed through the SEF to produce a correction factor. Figure 4 shows the kernel weights of SEF.

W×H is the width and height of the original grayscale secret image GI where GI(x, y)≥0 and GI(x, y)≤255. The following four steps are employed to create a semantic image SI. The size of the semantic image SI is W×H.

Step 1: Consider the pixel in GI(x, y) to be set as (1, 1).

Step 2: Compute the error value E(x, y) according to Eq. 1 for the pixel located at coordinates (x, y) in grayscale image GI:

$$E(x,y) = \text{Floor}\left(\frac{GI(x,y)}{100} + \frac{GI(x,y)}{10} \bmod 10 + GI(x,y) \bmod 10\right) \quad (1)$$

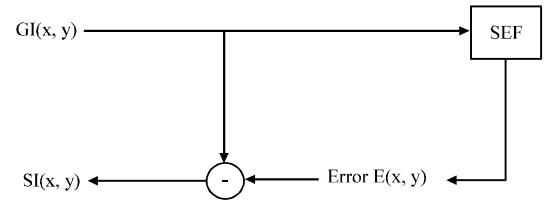

Fig. 3: Flowchart of error reduction

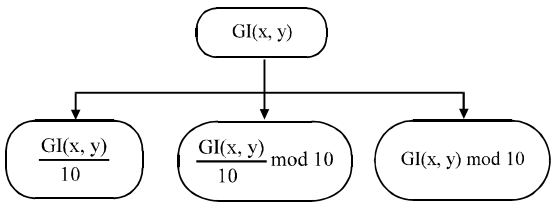

Fig. 4: Flowchart of semantic error filter strategy

Step 3: The modified values are computed according to Eq. 2 for the pixel located at coordinates (x, y) in grayscale image GI:

$$SI(x,y) = GI(x,y) - E(x,y) \quad (2)$$

Step 4: If x = H and y = W then stop and output the semantic image SI otherwise, go to step 2 and process the next pixel in the grayscale image GI.

Example for error reduction: A simple example is taken for explanation; this semantic image SI is generated by considering a GI as 3×3 matrix containing 9 pixels:

$$GI = \begin{bmatrix} 124 & 175 & 160 \\ 213 & 61 & 247 \\ 83 & 147 & 195 \end{bmatrix} \quad (3)$$

Step 1: Process the image pixel-wise; first pixel taken into consideration (Eq. 3) since N is 1:

$$GI(1,1) = [124] \quad (4)$$

Step 2: Compute the error value E(x, y) by using Eq. 1:

$$E(1,1) = [7] \quad (5)$$

Step 3: Reduce the error E(x, y) by using Eq. 2:

$$SI(1,1) = [117] \quad (6)$$

Step 4: Likewise, process the above steps until N = 9; the following semantic image SI∈{1, 2, ..., N} is generated based on error values E∈{1, 2, ..., N} (Eq. 7):

$$E = \begin{bmatrix} 7 & 13 & 7 \\ 6 & 7 & 13 \\ 11 & 12 & 15 \end{bmatrix} \quad SI = \begin{bmatrix} 117 & 162 & 153 \\ 207 & 54 & 234 \\ 72 & 135 & 180 \end{bmatrix} \quad (7)$$

MATERIALS AND METHODS

This study presents a detailed description of a novel SVCP called a Semantic Visual Cryptographic Protocol proposed for grayscale images. Figure 5 shows the proposed method for robust visual cryptography. In SVCP, encode the shares into meaningful covers and taking the meaningful secret information which does not allow the intruders to suspect the secret information. Generally, reconstructed secret image quality will reduce by pixel replacing and perceived errors. The goal is to

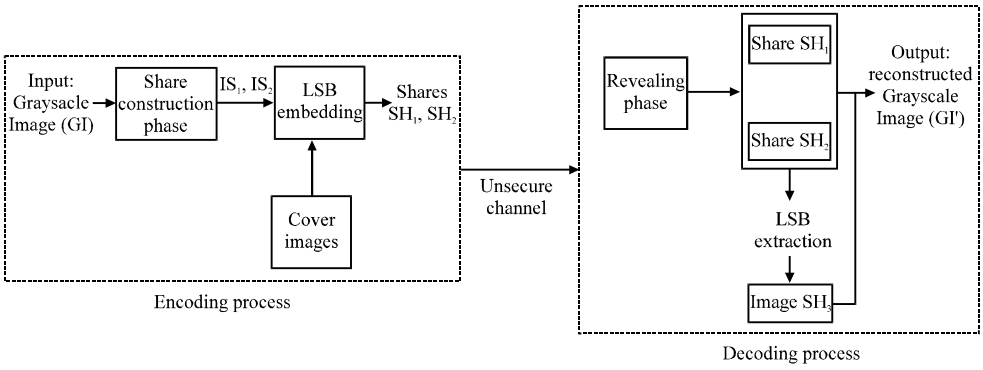

Fig. 5: Block diagram of proposed SVCP

reduce the perceived errors among the continuous-tone images with respect to grayscale visual cryptography. Complete details of the proposed scheme presented in two phases. First, share construction phase, which creates two shares from the secret image GI. Note that intermediate share IS3 will be retrieved from IS1 and IS2 in revealing phase. Then, construct the secret image from collection of shares.

Share construction phase:

Step 1: Consider a 512×512 secret Grayscale Image (GI) and meaningful grayscale image as the cover images (Eq. 8) then:

$$\begin{aligned} CI1_{i,j} &\in \{0,1,2,3...,255\} \\ CI2_{i,j} &\in \{0,1,2,3...,255\} \end{aligned} \tag{8}$$

where, i and j are varying from 1-512.

Step 2: Generate a Semantic Image (SI) by applying the error reduction technique on the grayscale image (Eq. 9):

$$\begin{aligned} GI_{i,j} &\in \{0,1,2,3...,255\} \\ SI_{i,j} &\in \{0,1,2,3...,255\} \end{aligned} \tag{9}$$

Step 3: Construct the intermediate shares $IS1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $IS2_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ from semantic image SI by using Eq. 10 now, the intermediate shares IS1 and IS2 has the pixel values ranging between 0 and 9:

$$\begin{aligned} IS1_{i,j} &\leftarrow SI_{i,j} \text{ Mode}/10 \\ IS2_{i,j} &\leftarrow SI_{i,j}/10 \end{aligned} \tag{10}$$

Step 4: Intermediate shares IS1 and IS2 can be embedded into cover images CI1 and CI2 by using the LSB embedding procedure (Chan and Cheng, 2004) to generate two shares SH1 and SH2. To complete the desired

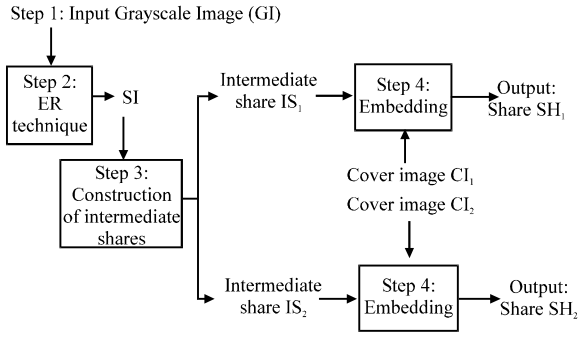

Fig. 6: Block diagram of share construction phase

experimental results, researchers chose the LSB embedding procedure (Chan and Cheng, 2004) because it not only provides high encoding capability but also assurance that the two shares and can be completely restored after stacked from the shares $SH1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $SH2_{i,j} \in \{0, 1, 2, 3, ..., 255\}$, respectively. Then, it will be delivered to the participants. Figure 6 shows the flowchart of share construction phase.

Revealing phase

Step 1: Get 512×512 share images $SH1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $SH_{i,j} \in \{0, 1, 2, 3, ..., 255\}$.

Step 2: By using the LSB extraction procedure (Chan and Cheng, 2004), the intermediate shares $IS1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $IS2_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ can be derived from share images. Now, IS1 and IS2 have the pixel values range between 0 and 9. By using Eq. 11, intermediate share IS3 can be derived from IS1 and IS2.

Step 3: To generate the reconstructed secret image GI', digitally stacking the intermediate shares IS1, IS2 and IS3 by using Eq. 11:

$$e = ISI_{i,j} + IS2_{i,j}$$
$$IS3_{i,j} = \begin{cases} 9\text{-}e & \text{if}(e < 9), \\ 1 & \text{if}(e > 9), \end{cases} \quad (11)$$
$$GI`_{i,j} = IS1_{i,j} + (IS2_{i,j} \times 100) + (IS3_{i,j} \times 10)$$

where, e is a varying integer value. Proposed SVCP can extend to color images. First, a color image will decompose into three sub-channel images: red, green and blue. Secondly, the scheme can apply independently to each sub-image, separately. Lastly, the reconstructed secret color image will generate by adding three channel images together.

RESULTS AND DISCUSSION

Experimental results demonstrate on two objectives. First reconstruct the original secret image with high quality; secondly, relate with no pixel expansion. The proposed SVCP allows no limitation on the size of the secret images. The set of test images shown in Fig. 7 illustrates that SVCP can perform well on grayscale images. The set contains eight 512×512 grayscale images: Lena, Baboon, Peppers, Airplane, Barbara, Fruits, Gold-hill and Elaine. The efficiency of the proposed method outlined in this study is tested by coding and running the algorithm in MATLAB 7.10 Tool. The image quality measures such as Normalized Correlation (NC), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Universal image Quality Index (UQI), Signal to Noise Ratio (SNR) and Mean Absolute Error (MAE) are evaluated between reconstructed images and original secret images using following equations.

Peak Signal to Noise Ratio (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is expressed in terms of the logarithmic decibel is given by Chan and Cheng (2004):

$$PSNR = \log \frac{(2^n\text{-}1)^2}{MSE} \quad (12)$$

Universal Quality Index (UQI): Universal quality index attempts to measure the quality of the image after the removal of the noise present in the image. The equation is given by Rajitha *et al*. (2012):

$$UQI = \frac{1}{N\text{-}1} \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \quad (13)$$

Here, $x = \{x_i | i = 1, 2 \ldots N\}$ and $y = \{y_i | i = 1, 2 \ldots N\}$ be the original and decrypted image signals, respectively.

Normalized Correlation (NC): It measures the similarity representation between the original image and decrypted image:

$$NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j]I'[i,j])}{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j])^2} \quad (14)$$

Fig. 7: Eight 512×512 grayscale images; a) Lena; b) Baboon; c) Peppers; d) Airplane; e) Barbara; f) Fruits; g) Gold-hill and h) Elaine

Where:
I(i, j) = Original image
I`(i, j) = Decrypted image
M = Height of image
N = Width of the image

Mean Square Error (MSE): It measures the average of the square of the error. The error is the amount by which the pixel value of the original image differs to the pixel value of the decrypted image (Liu and Wu, 2011):

$$MSE = \frac{\sum_{R,G,B}\sum_{i=1}^{M}\sum_{j=1}^{N}(I[i,j]-I'[i,j])^2}{3MN} \quad (15)$$

Here:
M and N = The height and width of the image, respectively
f(i, j) = The (i, j) pixel value of the original image
f (i, j) = The (i, j) pixel value of decrypted image

Signal to Noise Ratio (SNR): It is defined as the ratio of signal power to the noise power often expressed in decibels. The SNR is given by Ciptasari *et al.* (2014):

$$SNR = 10.\log 10\left[\frac{\sum_{0}^{n_x-1}\sum^{n_y-1}\left[r(x,y)\right]^2}{\sum_{0}^{n_x-1}\sum^{n_y-1}\left[r(x,y)-t(x,y)\right]^2}\right] \quad (16)$$

Here, $r = \{x_i|\ i = 1, 2 \ldots n\}$ and $t = \{y_i|\ i = 1, 2 \ldots n\}$ be the original and reconstructed image signals, respectively. Table 2 represents the computed values for image quality evaluation for the reconstructed images.

Mean Absolute Error (MAE): It is a capacity used to measure how nearby predictions are to the eventual consequences. The mean absolute error is given by:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|f_i - y_i| = \frac{1}{n}\sum_{i=1}^{n}|e_i| \quad (17)$$

Here, mean absolute error is an average of the absolute errors $e_i = |f_i - y_i|$, where f_i is the prediction and y_i the true value.

Figure 8a-f shows secret image Lena, cover images Goldhill, Barbara, Share 1, 2 and reconstructed secret image Lena. Share images are looking different from secret image therefore, this method can escape from visual attack.

The graph representation of the various image quality measures are shown in Fig. 9. The PSNR values of the reconstructed secret images and the original images range from 36-37.98 dB. By seeing the obtained PSNR, UQI, NC, MSE, SNR and MAE values, reconstructed grayscale images can be presumed to be absolutely believable. From

Table 2: Results of various images

Images	NC	PSNR (dB)	MSE	UQI	SNR (dB)	MAE
Lena	0.9962	37.88	10.73	0.9	3.7623	9.642
Baboon	0.9953	37.63	11.45	0.8	3.4233	10.041
Barbara	0.9967	37.25	10.38	0.9	3.8252	9.506
Elaine	0.9965	37.23	11.43	0.8	3.5495	9.902
Goldhill	0.9970	37.98	10.32	0.9	3.8893	9.460
Peppers	0.9972	36.50	12.17	0.8	3.0500	10.260

Fig. 8: a) Secret image Lena; b) cover image, Gold-hill; c) cover image, Barbara; d) share 1; e) share 2 and f) Reconstructed secret image, Lena

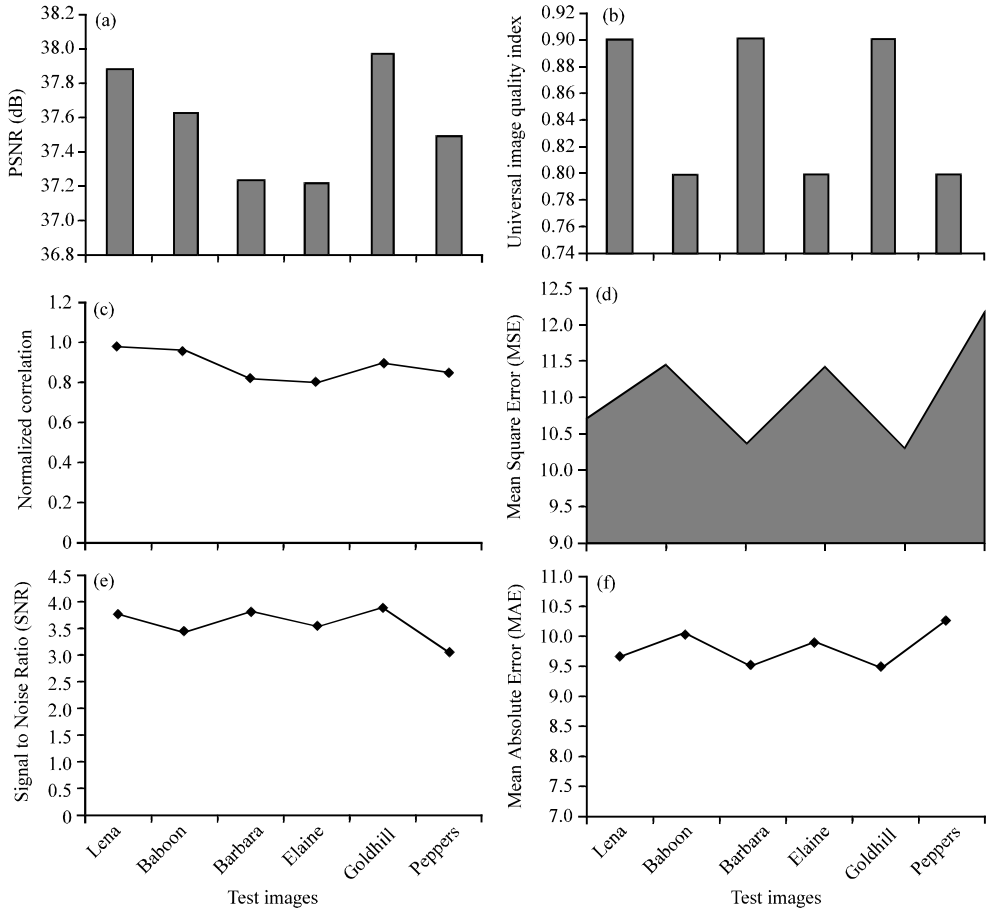

Fig. 9: Graph representation of reconstructed image quality measures; a) PSNR; b) UQI; c) NC; d) MSE; e) SNR and f) MAE

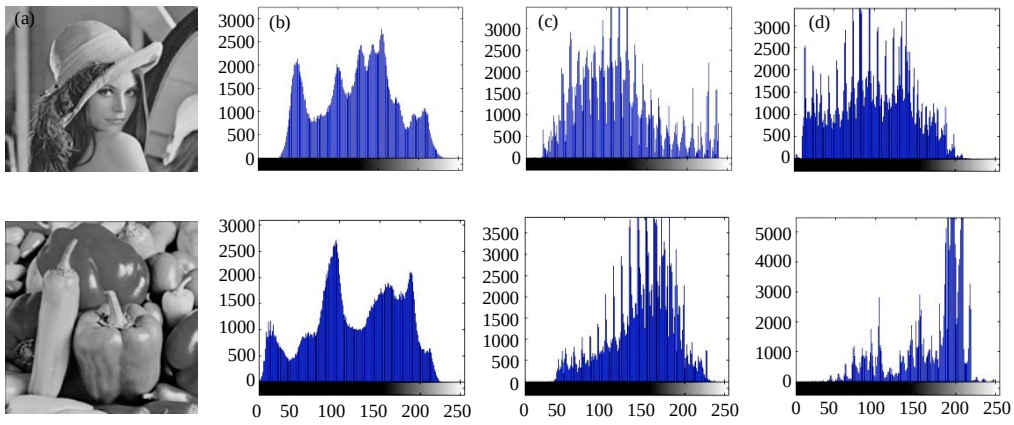

Fig. 10: Histogram of images; a) Secret image; b) Histrogarm of secrete image, c) Histrogarm of share 1, d) Histrogram of share 2

Researchers can see that the reconstructed image quality using SVCP is better than using Li (2007) scheme (Table 3). The difference between PSNRs generated with the scheme and by Li (2007) scheme is ranged from 9-10 dB.

Analysis of attack: Statistical attack is a widely used technique in cryptanalysis and hence an effective SVCP should be highly robust against any statistical attacks.Analyzing the histogram in the secret image and in the share images is the statistical analysis to prove the

Table 3: Reconstructed image quality of two schemes

Gray scale images	Wang *et al.* (2006) reconstructed image quality		Proposed reconstructed image quality	
	PSNR (dB)	NC	PSNR (dB)	NC
Lena	27.78	0.83	37.86	0.99
Peppers	27.36	0.82	37.30	0.99

robustness of the proposed SVCP against any statistical attack. Figure 10 shows the histogram of secret images and its share images. Share images are entirely different with the histogram of the secret image and do not provide any suitable information to employ a statistical attack.

CONCLUSION

Proposed Semantic Visual Cryptographic Protocol (SVCP) for the grayscale images which uses the error reduction. The use of error reduction technique improves the quality of encrypted image and decrypted image. The proposed protocol helps to generate high quality share images. An individual shares does not show the secret information. Future studies should therefore investigate on 3D visual secret sharing with higher visual quality of the reconstructed secret images.

ACKNOWLEDGEMENT

The research is supported by UGC, New Delhi for its financial assistance under UGC major research projects in Engineering and Technology on January 2013.

REFERENCES

Askari, N., H.M. Heys and C.R. Moloney, 2013. An extended visual cryptography scheme without pixel expansion for halftone images. Proceedings of the IEEE 26th Annual Canadian Conference on Electrical and Computer Engineering, May 5-8, 2013, Regina, SK., pp: 1-6.

Ateniese, G., C. Blundo, A. De Santis and D.R. Stinson, 1996. Visual cryptography for general access structures. Inform. Comput., 129: 86-106.

Babu, C.R., M. Sridhar and B.R. Babu, 2013. Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security. Proceedings of the International Conference on Information Systems and Computer Networks, March 9-10, 2013, Mathura, pp: 195-199.

Borchert, B., 2007. Segment based visual cryptography. Taubingen University, WSI -2007, Germany.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recogn., 37: 469-474.

Chang, C.C., C.C. Lin, T.H.N. Le and H.B. Le, 2009. Self-verifying visual secret sharing using error diffusion and interpolation techniques. IEEE Trans. Inform. Forensics Secur., 4: 790-801.

Ciptasari, R.W., K.H. Rhee and K. Sakurai, 2014. An enhanced audio ownership protection scheme based on visual cryptography. EURASIP J. Inform. Secur.,. 10.1186/1687-417X-2014-2.

Fang, L. and B. Yu, 2006. Research on pixel expansion of (2, n) visual threshold scheme. Proceedings of the IEEE International Symposium on Pervasive Computing and Apps, August 3-5, 2006, Urumqi, pp: 856-860.

Fridrich, J., 2009. Steganography in Digital Media: Principles, Algorithms and Applications. Cambridge University Press, Cambridge, England, ISBN-13: 978-0521190190, Pages: 462.

Ito, R., H. Kuwakado and H. Tanaka, 1999. Image size invariant visual cryptography. IEICE Trans. Fundam., E82-A: 2172-2177.

Lee, K.H. and P.L. Chiu, 2012. An extended visual cryptography algorithm for general access structures. IEEE Trans. Inform. Forensics Secur., 7: 219-229.

Li, L.C., 2007. Visual cryptography for meaningful shares. Master's Thesis, Institute of Communication Engineering, Tatung University.

Liu, F. and C. Wu, 2011. Embedded extended visual cryptography schemes. IEEE Trans. Inform. Forensics Secur., 6: 307-322.

Lukac, R. and K.N. Plataniotis, 2005. Bit-level based secret sharing for image encryption. Pattern Recognit., 38: 767-772.

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

Naor, M. and A. Shamir, 1994. Visual cryptography. Adv. Cryptol., 950: 1-12.

Rajitha, T., P.P. Kumar and V. Laxmi, 2012. Construction construction of extended visual cryptography of extended visual cryptography of extended visual cryptography scheme secret sharing for secret sharing. Int. J. Comput. Sci. Network, 1: 85-90.

Wang, Z., G.R. Arce and G. Di Crescenzo, 2009. Halftone visual cryptography via error diffusion. IEEE Trans. Inform. Forensics Secur., 4: 383-396.

Wang, Z.M., G.R. Arce and G. Di Crescenzo, 2006. Halftone visual cryptography via direct binary search. Proceedings of the 14th European Signal Processing Conference, September 4-8, 2006, Florence, Italy.

Wu, C.C., 1998. A study on visual cryptography. Master Thesis, National Chiao Tung University, Taiwan, China.