Asian Journal of Information Technology 13 (9): 506-512, 2014
ISSN: 1682-3915
© Medwell Journals, 2014

Multi-Secret Semantic Visual Cryptographic Protocol (MSVCP) for Securing Image Communications

A. John Blesswin and P. Visalakshi
Department of Electronics and Communication Engineering,
PSG College of Technology, 641004 Coimbatore, India

Abstract: Visual cryptography is one of the ways, to share the visual secret information securely. Visual Cryptography Scheme (VCS) is an Encryption Method which provides information security that uses combinatorial techniques to encode secret written materials without any Complex Cryptographic algorithms. Researchers propose a new Multi-secret based Semantic Visual Cryptographic Protocol (MSVCP) that can encode the two secret images into the shares using error reduction. 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 proposed a novel scheme called a MSVCP which can be applied to grayscale images. The experimental result shows the effectiveness and advantages of the proposed MSVCP and it ensures the security and quality of the reconstructed secret images.

Key words: Communications, Visual Cryptography Scheme (VCS), MSVCP, encode, image

INTRODUCTION

Image Security (IS) is one of the key focus areas of Medical Image Communication (MIC). MIC over wide networks has become popular with the fast development of the internet technology and high-speed networks. However, there are two levels of communications in MIC. First, medical image communication in local area networks; it will be protected by internal firewall. Secondly, communication over from the local area network; it may bring lot of chances to the intruder to steal the secret information in public networks. Therefore, protection of the reliability and privacy of the medical images is an important issue. Encryption is the good technique to assure information security during its transmission through public networks (Fridrich, 2009). Conventional methods are securing the medical images by steganography or watermarking techniques. To encrypt the entire medical image by using conventional methods, it was more computational complexity and time-consuming process. Visual Cryptography (VC) is a new encryption technique used in the secure transfer of images and solves the problems of computational complexity. To describe the principles of Visual Secret Sharing (VSS), consider a model by Noar and Shamir (1995) VC scheme as shown in Table 1. The idea of their VC scheme is to generate two share images by the combinations of black and white pixels according to the secret image. Naor and Shamir's Model was expanded to general access structure by Ateniese *et al.* (1996). They designed a novel technique to bring k out of n visual cryptography schemes. It is unable to obtain any secret information by stacking less number of favorable shares. Wu (1998) invented a VC scheme to share more than one secret image in two random shadows. Ito *et al.* (1999) minimized the share image size by 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 are applied to accomplish the work of generating shares.

Table 1: Construction of (2, 2) VC scheme

Images	White pixel	Black pixel
Share 1	◧◨	◧◨
Share 2	◧◨	◨◧
Share 1×2	◧◨	■■

First color visual cryptography scheme was introduced by Verheul and Tilborg (1997) where each color image is converted into RGB channels where each channel contains the pixel value of range between 0 and 255. Kumari and Bhatia (2010) found Stucki kernel to increase the visual quality of the color halftone images by adding the additional pixel patterns. Askari *et al.* (2013) proposed the extended visual cryptography, the share images are constructed to contain meaningful cover

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

images, thereby providing opportunities for integrating visual secret sharing scheme and biometric security techniques. Babu *et al.* (2013) proposed information hiding in grayscale images using Pseudo-Randomized Visual Cryptography algorithm for visual information security. Researchers proposed the new Multi-secret Semantic Visual Cryptographic Protocol (MSVCP) to transfer multi-secret medical images in secure way. The reconstructed medical images obtained must be kept back completely without any loss of information. The research is focused on three paths:

- Sharing two secret medical images with good operational efficiency
- Shares should look like a meaningful nature image (confidentiality)
- Reconstruct the medical image with high quality

The review of Multi-secret Semantic Visual Cryptography Protocol (MSVCP) is structured as follows.

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. 1. 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 2 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:

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

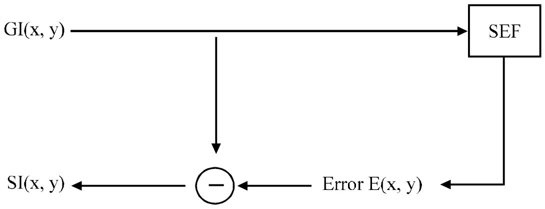

Fig. 1: Flowchart of error reduction

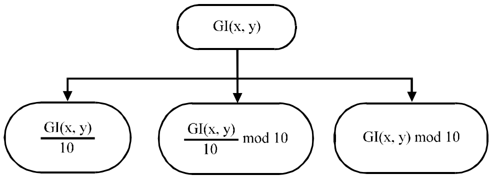

Fig. 2: Flowchart of semantic error filter strategy

- 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 in 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):

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

MATERIALS AND METHODS

This study proposes an introduced system of sharing the medical images in a secure way. In MSVCP, encode the shares into nature cover images and do not draw attention which keeps them confidential. The basic idea of MSVCP proposed system described in two phases. First, share construction phase which creates two shares SH1 and SH2 from the secret medical image MI. Note that intermediate shares IS13 and IS23 will be retrieved from IS1 and IS2 in revealing phase. Secondly, reconstruct the secret medical image MI` from collection of shares SH1 and SH2. Figure 3 describes a general MSVCP methodology as listed as.

Share construction phase: This study describes the procedure of generating shares from secret medical image MI and it will be shared among to the participants. Each pixel of single medical image $MI_{i,\ j}$ corresponds to one pixel in share images $SH1_{i,\ j}$ and $SH2_{i,\ j}$. Secret image is processed one pixel at a time in share construction phase. The dealer should select two natural looking cover images $CI1_{i,\ j}$, $CI2_{i,\ j}$ of size W×H to encode a two secret medical image for a proposed secret sharing scheme.

Step 1: Consider a two 512×512 secret medical grayscale image (MI) of size W×H pixel Eq. 8 and two nature grayscale image as the cover images (Eq. 2):

$$\begin{aligned} & MI1_{i,j} \in \{0,1,2,3\ldots,255\} \\ & MI2_{i,j} \in \{0,1,2,3\ldots,255\} \\ & CI1_{i,j} \in \{0,1,2,3\ldots,255\} \\ & CI2_{i,j} \in \{0,1,2,3\ldots,255\} \end{aligned} \qquad (8)$$

where, i and j are varying from 0-255.

Step 2: Generate a two Semantic Images (SI) by applying the error reduction technique on two medical grayscale images $MI1_{i,\ j}$ and $MI2_{i,\ j}$ Eq. 9:

$$\begin{aligned} & SI1_{i,j} = ER(MI1_{i,j}) \\ & SI2_{i,j} = ER(MI2_{i,j}) \\ & SI1_{i,j} \in \{0,1,2,3\ldots,255\} \\ & SI2_{i,j} \in \{0,1,2,3\ldots,255\} \end{aligned} \qquad (9)$$

Step 3: Construct the intermediate shares $IS11_{i,\ j} \in \{0, 1, 2, 3, ..., 255\}$ and $ISI2_{i,\ j} \in \{0, 1, 2, 3, ..., 255\}$ from semantic image $SI1_{i,\ j}$ then $IS21_{i,\ j} \in \{0, 1, 2, 3, ..., 255\}$ and $IS22_{i,\ j} \in \{0, 1, 2, 3, ..., 255\}$ from semantic image $SI2_{i,\ j}$ by using Eq. 10; the intermediate shares $IS11_{i,\ j}$, $IS12_{i,\ j}$, $IS21_{i,\ j}$ and $IS22_{i,\ j}$ pixel values ranging between 0 and 9:

$$\begin{aligned} & IS11_{i,j} \leftarrow Mod(SI1_{i,j}, 10) \\ & IS12_{i,j} \leftarrow SI1_{i,j}/10 \\ & IS21_{i,j} \leftarrow Mod(SI2_{i,j}, 10) \\ & IS22_{i,j} \leftarrow SI2_{i,j}/10 \end{aligned} \qquad (10)$$

Step 4: Intermediate shares $IS11_{i,\ j}$, $IS12_{i,\ j}$, $IS21_{i,\ j}$ and $IS22_{i,\ j}$ can be embedded into cover images CI1 and CI2 by using the Least Significant Bit (LSB) embedding procedure (Babu *et al*., 2013) to generate two shares $SH1_{i,\ j}$ and $SH2_{i,\ j}$ Eq. 11. The shares size will be 2W×H. To complete the desired experimental results, researchers chose the LSB embedding procedure (Kim *et al*., 2008) 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 clinician participants:

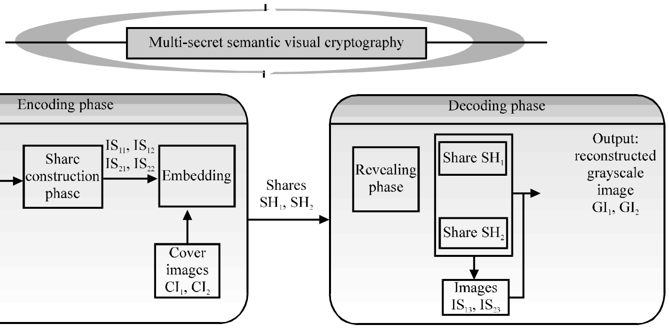

Fig. 3: Block diagram of proposed MSVCP

$$\begin{aligned} &SH1(i, (2*j-1)) \leftarrow CI1_{i,j} + IS11_{i,j} \\ &SH1(i, (2*j)) \leftarrow CI1_{i,j} + IS21_{i,j} \\ &SH2(i, (2*j-1)) \leftarrow CI2_{i,j} + IS12_{i,j} \\ &SH2(i, (2*j)) \leftarrow CI2_{i,j} + IS22_{i,j} \end{aligned} \tag{11}$$

Reconstruction phase: The clinician participants collect their share images $SH1_{i,j}$ and $SH2_{i,j}$ in the reconstruction phase to reconstruct the secret medical image MI`. Two shares will be enough to reconstruct the secret medical image $MI1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $MI2_{i,j} \in \{0, 1, 2, 3, ..., 255\}$.

Step 1: Get 512×512 share images $SH1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $SH2_{i,j} \in \{0, 1, 2, 3, ..., 255\}$.

Step 2: By using the LSB extraction procedure (Kim *et al.*, 2008), $ISI1_{i,j} \in \{0, 1, 2, 3, ..., 255\}$and $IS21_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ can be derived from share $SH1_{i,j}$. Similarly, $IS12_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ and $IS22_{i,j} \in \{0, 1, 2, 3, ..., 255\}$ can be derived from share $SH2_{i,j}$. Now, IS1 and IS2 have the pixel values range between 0 and 9. By using Eq. 12, intermediate shares $IS13_{i,j}$ and $IS23_{i,j}$ can be derived from IS1 and IS2:

$$\begin{aligned} e1 &= IS11_{i,j} + IS12_{i,j} \\ e2 &= IS21_{i,j} + IS22_{i,j} \end{aligned}$$

where, i and j are varying from 0-255:

$$IS13_{i,j} = \begin{cases} 9-e1 & if(e1<9) \\ 1 & if(e>9) \\ 0 & otherwise \end{cases} \tag{12}$$

where, e1 is varying integer value:

$$IS23_{i,j} = \begin{cases} 9-e2 & if(e2<9) \\ 1 & if(e2>9) \\ 0 & otherwise \end{cases}$$

where, e2 is varying integer value.

Step 3: Value of $IS13_{i,j}$ and $IS23_{i,j}$ will be used to recover the secret medical image pixel values. To generate the reconstructed secret image MI`, digitally stacking the intermediate shares IS1, IS2 and IS3 by using in Eq. 13:

$$\begin{aligned} MI1`_{i,j} &= IS11_{i,j} + (IS12_{i,j} \times 10) + (IS13_{i,j} \times 100) \\ MI2`_{i,j} &= IS21_{i,j} + (IS22_{i,j} \times 10) + (IS23_{i,j} \times 100) \end{aligned} \tag{13}$$

Proposed MSVCP can extend to Digital Imaging and Communications in Medicine (DICOM) medical images. First, a DICOM image will convert into Joint Photographic Experts Group (JPEG) format. JPEG color image will decompose into three sub-channel images: red, green and blue. Secondly, the proposed MSVCP can apply independently to each sub-image, separately. Lastly, the reconstructed secret image will generate by adding three channel images together; then, it will be converted into DICOM format. Thus, it is easy for clinicians to reconstruct the medical images.

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 MSVCP allows no limitation on the size of the secret images. MSVCP can perform well on grayscale images. The efficiency of the proposed method is testing by coding and running the algorithm in MATLAB 7.10 Tool.

The image quality measures such as Image Quality Index (IQI), 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 Chang *et al.* (2009):

$$PSNR = \log \frac{(2^n - 1)^2}{MSE} \tag{14}$$

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. Equation 15 is given by Babu *et al.* (2013):

$$UQI = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \tag{15}$$

Where:
$x = \{x_i \mid i = 1, 2 \ldots N\}$ be the original image signals
$y = \{y_i \mid i = 1, 2 \ldots N\}$ be the decrypted image signals

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

$$\mathrm{NC}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I[i,j]I'[i,j])}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I[i,j])^2} \tag{16}$$

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 (Chang *et al*., 2009):

$$\mathrm{MSE}=\frac{\sum_{R,G,B}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I[i,j]-I'[i,j]\right)^2}{3MN} \tag{17}$$

Where:

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

Table 2: Results of various images

Images	NC	PSNR(dB)	MSE	UQI	SNR(dB)	MAE
Lena	0.9962	37.86	10.73	0.82	3.7623	9.642
Baboon	0.9953	37.52	11.52	0.93	3.4233	10.041
Barbara	0.9967	37.95	10.41	0.87	3.8252	9.506
Elaine	0.9965	37.64	11.26	0.90	3.5495	9.902
Fruit	0.9965	37.26	12.28	0.88	3.1701	10.440
Goldhill	0.9970	37.98	10.41	0.90	3.8893	9.460
Line	0.9934	36.85	13.51	0.41	2.7580	10.620
Peppers	0.9972	37.30	12.17	0.85	3.0500	10.260

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):

$$\mathrm{SNR}=10.\log 10\left[\frac{\sum_{0}^{n_x-1}\sum^{n_y-1}\left[r(x,y)\right]^2}{\sum_{0}^{n_x-1}\sum^{n_y-1}\left[r(x,y)-t(x,y)\right]^2}\right] \tag{18}$$

Where:

$r = \{x_i| \; i = 1, 2 \ldots n\}$ be the original image signals
$t = \{y_i| \; i = 1, 2 \ldots n\}$ be the reconstructed image signals

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:

$$\mathrm{MAE}=\frac{1}{n}\sum_{i=1}^{n}\left|f_i-y_i\right|=\frac{1}{n}\sum_{i=1}^{n}\left|e_i\right| \tag{19}$$

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

Figure 4a-h show secret image Lena, pepper, cover images baboon, barbara, share 1, share 2 and reconstructed secret image Lena and pepper. Share images are looking different from secret image therefore, this method can escape from visual attack.

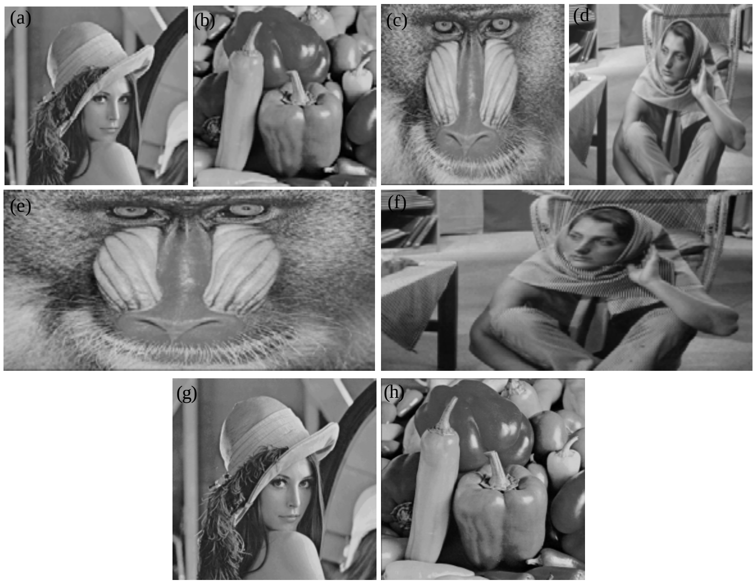

Fig. 4: a) Secret image, Lena; b) secret image, pepper; c) cover image, baboon; d) cover image, barbara; e) share 1; f) share 2; g) Reconstructed secret image, Lena and h) reconstructed secret image, pepper

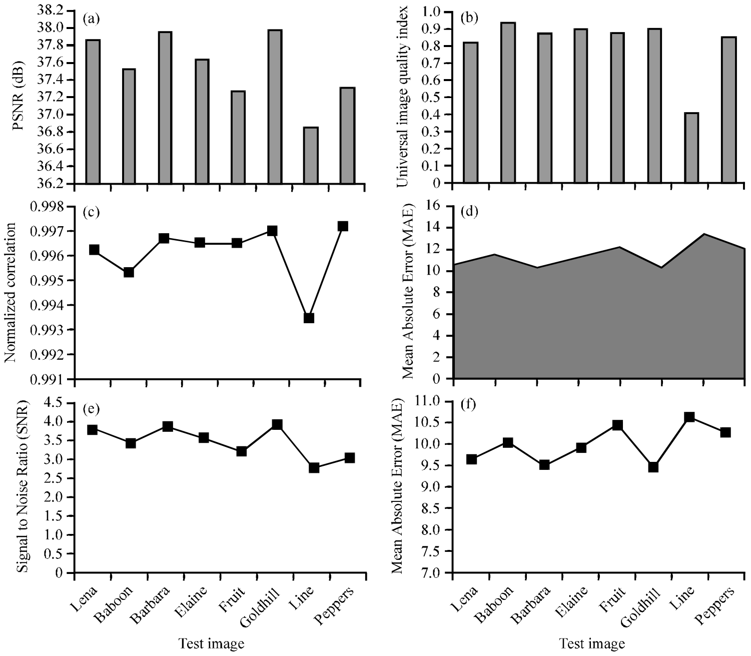

Fig. 5: Graph representation of reconstructed image quality measures; a) PSNR; b) UQI; c) NC; d) MSE; e) SNR and f) MAE

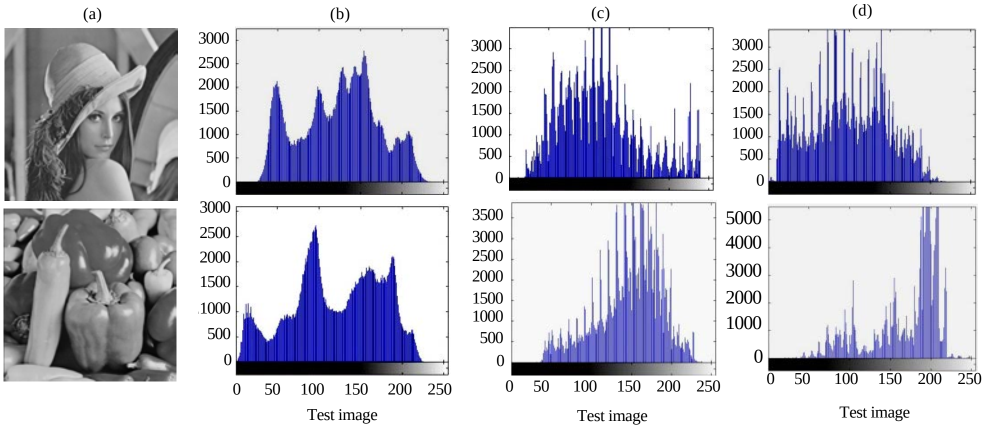

Fig. 6: Histogram of images; a) secret image; b) histogram of secret image; c) histogram of share 1 and d) histogram of share 2

Figure 5 shows the graph representation of the various image quality measures. 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 presume to be believable. From Table 3, researchers can see that the reconstructed image quality using MSVCP is better than using Li (2007) scheme. The difference between PSNRs generated with the scheme and by Li (2007) scheme is ranging from 9-10 dB.

Table 3: Reconstructed image quality of two schemes

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

Analysis of attack: Analyzing the histogram in the secret image and in the share images is the statistical analysis to prove the robustness of the proposed MSVCP against any statistical attack. Figure 6 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 Multi-Secret Semantic Visual Cryptographic Protocol (MSVCP) 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.

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.

Fridrich, J., 2009. Steganography in Digital Media: PrinciplesSteganography In Digital Media: Principles, Algorithms and Applications. Cambridge University Press, Cambridge, England.

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

Kim, H.J., V. Sachnev, Y.Q. Shi, J. Nam and H.G. Choo, 2008. A novel difference expansion transform for reversible data embedding. IEEE Trans. Inform. Forensics Security, 3: 456-465.

Kumari, K. and S. Bhatia, 2010. Multi-pixel visual cryptography for color images with meaningful shares. Int. J. Eng. Sci. Technol., 2: 2398-2407.

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

Noar, M. and A. Shamir, 1995. Visual Cryptography. In: Advance in Cryptography: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques Perugia, De Santis, A. (Ed.). Springer, Netherlands, ISBN: 9783540601760, pp: 1-12.

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.

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