Multi-secret Semantic Visual Cryptographic Protocol for Securing Image Communications

A. John Blesswin[1], P. Visalakshi[2], R. Sivakumar[3], M. Karnan[4], J. Subash Chandra Bose[5]

Fulltime Research Scholar[1], Associate Professor[2]
PSG College of Technology, Coimbatore, India
[3,4]Professor, Tamilnadu College of Engineering, Coimbatore, India
[5] Associate Professor, Professional Group of Institutions, Palladam, 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. We 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.

I. Introduction

Image Security (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 [6].

Visual Cryptography (VC) is a new encryption technique used in the secure transfer of images and solves the problems of computational complexity. Naor and Shamir [1] 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 G. Ateniese et al [2]. 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. Kumari et al [7] found Stucki kernel to increase the visual quality of the color halftone images by adding the additional pixel patterns. Askari et al [8] proposed the extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual secret sharing scheme and biometric security techniques. Babu C.R et al [9] proposed information hiding in grayscale images using pseudo-randomized visual cryptography algorithm for visual information security. We 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 review of Multi-secret Semantic Visual Cryptography Protocol (MSVCP) is structured as follows. In Section II, we briefly review the error reduction technique, which adapted in proposed MSVCP. Complete details of our proposed MSVCP are explained in Section III. Section IV gives experimental results. Conclusions are presented in Section V.

II. Related Work

A. Error Reduction (ER)

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.

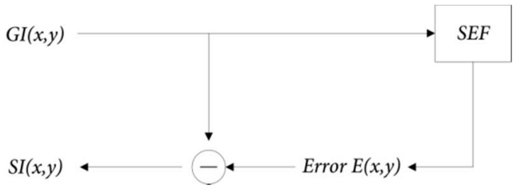

Figure 1. Flowchart of Error reduction

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 Figure 1. In this section, we 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.

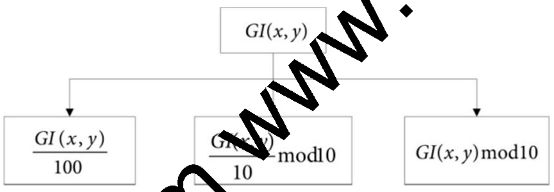

Figure 2. Flowchart of semantic error filter strategy

W × *H* is the width and height of the grayscale secret image GI. 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 (1) for the pixel located at coordinates (x, y) in grayscale image GI,

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

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

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

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.

III. proposed Methodology

This study proposes an introduced system of sharing the medical images in a secure way. 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 image MI` from collection of shares SH1 and SH2.

A. Share Construction Phase

This section 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. Figure 3 describes a general MSVCP methodology as listed below:

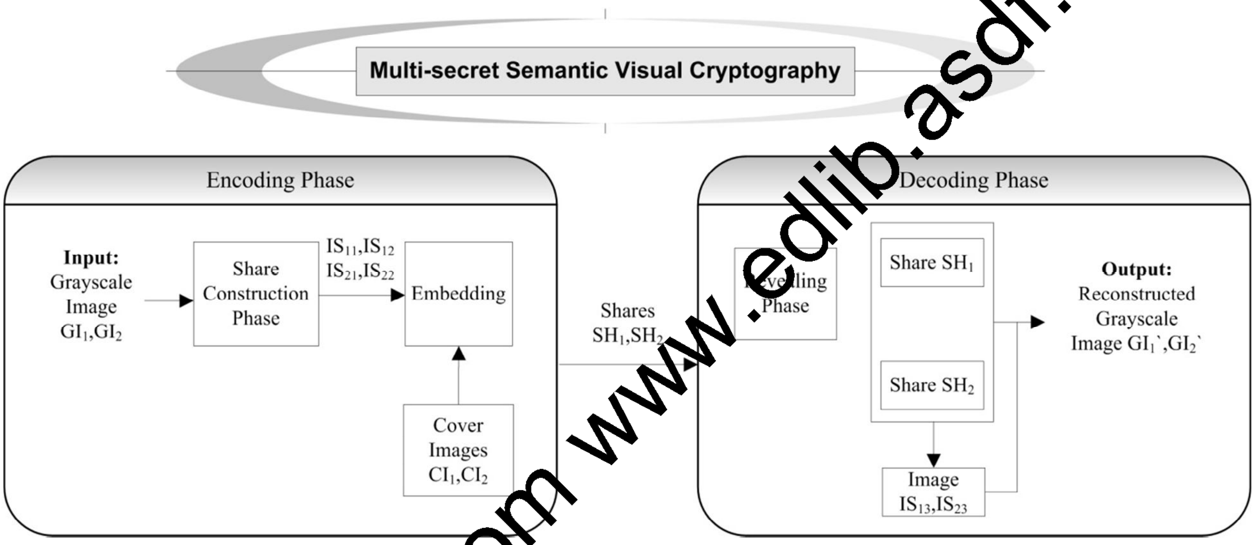

Figure 3. Block diagram of proposed MSVCP

Step 1. Consider a two 512×512 secret medical grayscale image (MI) of size *W*×*H* pixel (3) and two nature grayscale image as the cover images (2),

$$MI1_{i,j} \in \{0,1,2,3\ldots,255\} \,\&\, MI2_{i,j} \in \{0,1,2,3\ldots,255\} \,\&\, CI1_{i,j} \in \{0,1,2,3\ldots,255\} \,\&\, CI2_{i,j} \in \{0,1,2,3\ldots,255\} \quad (3)$$

Where i and j are varying from 0 to 255.

Step 2. Generate a two Semantic Images (SI) by applying the error reduction technique on two medical grayscale images $MI1_{i,j}$ and $MI2_{i,j}$ (4);

$$SI1_{i,j} = ER(MI1_{i,j}) \,\&\, SI2_{i,j} = ER(MI2_{i,j}) \,\&\, SI1_{i,j} \in \{0,1,2,3\ldots,255\} \,\&\, SI2_{i,j} \in \{0,1,2,3\ldots,255\} \quad (4)$$

Step 3. Construct the intermediate shares $IS11_{i,j} \in \{0,1,2,3\ldots,255\}$ and $IS12_{i,j} \in \{0,1,2,3\ldots,255\}$ from semantic image $SI1_{i,j}$ then $IS21_{i,j} \in \{0,1,2,3\ldots,255\}$ and $IS22_{i,j} \in \{0,1,2,3\ldots,255\}$ from semantic image $SI2_{i,j}$ by using (5); the intermediate shares $IS11_{i,j}, IS12_{i,j}, IS21_{i,j}, IS22_{i,j}$ pixel values ranging between 0 and 9.

$$\begin{aligned} IS11_{i,j} &\longleftarrow Mod(SI1_{i,j},10) \,\&\, IS12_{i,j} \longleftarrow SI1_{i,j}/10 \\ IS21_{i,j} &\longleftarrow Mod(SI2_{i,j},10) \,\&\, IS22_{i,j} \longleftarrow SI2_{i,j}/10 \end{aligned} \quad (5)$$

Step 4 .Intermediate shares $IS11_{i,j}, IS12_{i,j}, IS21_{i,j}, IS22_{i,j}$ can be embedded into cover images CI1 and CI2 by using the Least Significant Bit (LSB) embedding procedure [4], to generate two shares $SH1_{i,j}$ and $SH2_{i,j}$ (6).

The shares size will be $2W \times H$. To complete the desired experimental results, we chose the LSB embedding procedure [4], because it not only provides high encoding capability, but also assurance that our two shares and can be completely restored after stacked from the shares $SH1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $SH2_{i,j} \in \{0,1,2,3\ldots,255\}$ respectively. Then, it will be delivered to the clinician participants.

$$\begin{aligned} &SH1(i,(2*j-1)) \longleftarrow CI1_{i,j} + IS11_{i,j} \ \& \ SH1(i,(2*j)) \longleftarrow CI1_{i,j} + IS21_{i,j} \\ &SH2(i,(2*j-1)) \longleftarrow CI2_{i,j} + IS12_{i,j} \ \& \ SH2(i,(2*j)) \longleftarrow CI2_{i,j} + IS22_{i,j} \end{aligned} \tag{6}$$

B. 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 $MI1_{i,j} \in \{0,1,2,3\ldots,255\}$ and $MI2_{i,j} \in \{0,1,2,3\ldots,255\}$

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

Step 2. By using the LSB extraction procedure [7], $IS11_{i,j} \in \{0,1,2,3\ldots,255\}$ and $IS21_{i,j} \in \{0,1,2,3\ldots,255\}$ can be derived from share $SH1_{i,j}$. Similarly, $IS12_{i,j} \in \{0,1,2,3\ldots,255\}$ and $IS22_{i,j} \in \{0,1,2,3\ldots,255\}$ can be derived from share $SH2_{i,j}$. Now, IS1 and IS2 have the pixel values range between 0 and 9. By using (7), (8), (9), intermediate shares $IS13_{i,j}$ and $IS23_{i,j}$ can be derived from IS1 and IS2.

$$\begin{aligned} e1 &= IS11_{i,j} + IS12_{i,j} \\ e2 &= IS21_{i,j} + IS22_{i,j} \end{aligned} \tag{7}$$

Where i and j are varying from 0 to 255

$$IS13_{i,j} = \begin{cases} 9-e1 & if\,(e1<9), \\ 1 & if\,(e>9), \\ 0 & otherwise, \end{cases} \tag{8}$$

Where $e1$ is varying integer value

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

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 (10);

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

IV. Experimental Results

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) [5], Mean

Square Error (MSE) [3], Universal image Quality Index (UQI), Signal to Noise Ratio (SNR) [9] and Mean Absolute Error (MAE) are evaluated between reconstructed images and original secret images.

.

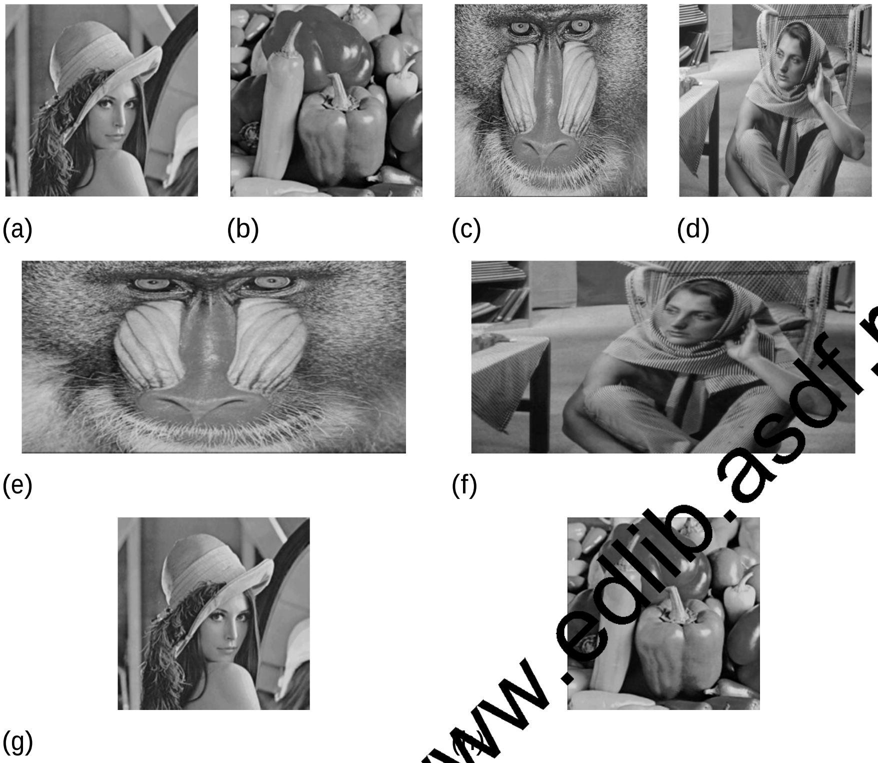

Figure 4. (a) Secret image, Lena (b) Secret image, Pepper (c) Cover image, Baboon (c) Cover image, Barbara (d) Share1 (e) Share2 (f) Reconstructed secret image, Lena (g) Reconstructed secret image, Pepper

Table I Results of Various Images

Image	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	10.44
Goldhill	0.9970	37.98	10.41	0.90	3.8893	9.46
Line	0.9934	36.85	13.51	0.41	2.7580	10.62
Peppers	0.9972	37.30	12.17	0.85	3.0500	10.26

Table I represents the computed values for image quality evaluation for the reconstructed images. Figures 4(a), 4(b), 4(c), 4(d), 4(e), 4(f), 4(g) and 4(h) shows secret image Lena, pepper, cover images Baboon, Barbara, Share1, Share2 and reconstructed secret image Lena and Pepper. Share images are looking different from secret image; therefore, this method can escape from visual attack. The PSNR values of the reconstructed secret images and the original images range from 36 to 37.98 dB. By seeing, the obtained PSNR, UQI, NC, MSE, SNR, and MAE values, reconstructed grayscale images can presume to be believable.

V. 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.

References

[1]. M. Naor and A. Shamir, “Visual cryptography," Proc. *Advances in Cryptology* (Eurprocrypt'94), pp.1 -12, 1994

[2]. G. Ateniese, C. Blundo, A. DeSantis, D. R. Stinson, *Visual cryptography for general access structures* Proc. *ICALP* 96, Springer, Berlin, pp.416-428, 1996

[3]. Li, Ling Chen, Shuenn-Shyang Wang, Visual Cryptography for meaningful shares, Thesis for master science, Institute of communication engineering, Tatung University, 2007

[4]. H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, “A novel difference expansion transform for reversible data embedding,” *IEEE Transactions of Information Forensics Security*, vol. 3, no. 3, pp. 456–465, Sep. 2008

[5]. Chin-Chen Chang, Fellow, IEEE, Chia-Chen Lin, Member, IEEE, T. Hoang Ngan Le, and Hoai Bac Le, "Self-Verifying Visual Secret Sharing Using Error Diffusion and Interpolation Techniques," *IEEE Information Forensics and security*, Vol. 4, No. 4, Dec 2009

[6]. J. Fridrich, “Steganography in Digital Media: Principles,” Algorithms, and Applications, Cambridge, England: Cambridge University Press; 2009

[7]. Kiran Kumari, Shalini Bhatia, Multi-pixel Visual Cryptography for color images with Meaningful Shares," International Journal of Engineering Science and Technology, Vol. 2(6), pp: 2398-2407, 2010

[8]. Askari, N.; Heys, H.M.; Moloney, C.R, "An extended visual cryptography scheme without pixel expansion for halftone images," Electrical and Computer Engineering (CCECE), 2013 26th Annual IEEE Canadian Conference, page(s): 1-6, 2013

[9]. Babu C.R, Sridhar, Babu B.R, "Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security," ISCON 2013 International Conference, Page(s): 195-199, 2013