I J C T A, 9(2) 2016, pp. 1055-1062

Optimal Visual Secret Sharing on Electrocardiography Images for Medical Secret Communications

A. John Blesswin[1*] and P. Visalakshi[2]

ABSTRACT

This work presents a Visual Cryptography (VC) method to share medical images. Visual Secret Sharing (VSS) is a model of cryptography which prevents the secret image from being destructed, and the secret image can be reconstructed by stacking the valid share images without complex computations. The proposed Optimal Visual Secret Sharing (OVSS) scheme converts the color image I into semantic image SI. Thus, noise initiated by the encoded secret pixel can totally be reduced; which helps to decrease the encoding complexity without affecting the quality. Then encrypts the SI into n shares and hide into the cover images called Stego-shares. In the revealing side, reconstruct the secret image from the collection of shares S1 and S2, without showing any interference with the Stego-shares. OVSS does not required pixel expansion. The experimental result explains the efficiency of the proposed OVSS, and it ensures the quality of the reconstructed images.

Keywords: Visual Cryptography, Secret sharing, Shares, Medical Communications, Security

INTRODUCTION

Visual Cryptography (VC) is one of the methods, to share the secret visual information securely. The share images contain the patterns of black and white pixel combinations. For the efficient management of visual cryptography, lots of schemes are developed by the researchers. Naor and Shamir's [1] VC scheme is to generate multiple shares by the combinations of black and white pixels according to the secret image. G. Ateniese et al. [2] expanded Naor and Shamir's model to general access structure. They designed a novel technique to bring k out of n visual cryptography schemes. Kai-Hui Lee [3] proposed (n,n)- VC scheme that can share one secret image over n-1 arbitrary selected natural shares with one noise-like share.

In this paper, we proposed an efficient OVSS protocol for grayscale images. OVSS applies to digital and printed media too. The feasible ways to hide the generated share are also discussed. The proposed OVSS not only has easier manageability but also reduces communication risk. In OVSS, the natural cover images will be gray of photographs, web images, etc. [6]. To minimize the communication risk the share is concealed behind the natural cover image with a different appearance by the information. When the communication cost is limited, the proposed scheme using unchanged cover images can significantly reduce the communications risk [6].

MATERIALS AND METHODS

This section presents a detailed description of a novel OVSS, called an Optimal Visual Secret Image Sharing scheme proposed for color medical images. OVSS encode the share images into natural covers and taking

[1] Assistant Professor, [2]Professor
[1] Department of Computer Science and Engineering, SRM University, India
[1] Department of Electronics and Communication Engineering, PSG College of Technology, India
E-mail: wjohnbless@gmail.com

the meaningful secret information, which does not allow the unauthorized user to suspect the secret information [8]. The proposed OVSS includes two main phases. Firstly, sharing and embedding phase creates two shares from the secret image GI. Natural cover images C1 and C2 [7] covers the intermediate shares IS1 and IS2. Secondly, revealing phase reconstructs the secret image from the collection of shares S1 and S2 using RNG procedure.

Sharing and embedding phase

This section describes a detailed algorithm for the sharing and embedding phase. A general flowchart of the sharing and embedding phase of our scheme appears in Figure 1. The color image is decomposed into Red, Green, and Blue (RGB) channels. From these channels the shares S1 and S2 are created using following steps:

Input: The secret color image I and cover image CI1, CI2.

Output: Stego-Shares S1, S2**.**

Step 1: Consider a 512 × 512 secret color image (I) and natural color image as the cover images CI_1 and CI_2 (1); then,

$$\begin{aligned} &[I] \rightarrow RGB \rightarrow I^R, I^G, I^B \\ &[CI_1] \rightarrow RGB \rightarrow CI_1{}^R, CI_1{}^G, CI_1{}^B \\ &[CI_2] \rightarrow RGB \rightarrow CI_2{}^R, CI_2{}^G, CI_2{}^B \\ &I, CI_1, CI_2 \in \{0,1,2,3\ldots,255\} \end{aligned} \tag{1}$$

Step 2: Generate a semantic image (SI) by applying the error reduction technique [13] on the secret color image (2);

$$\begin{aligned} &I^R, I^G, I^B \rightarrow ER \rightarrow SI^R, SI^G, SI^B \\ &SI^R, SI^G, SI^B \in \{0,1,2,3\ldots,255\} \end{aligned} \tag{2}$$

Step 3: Construct the intermediate shares $IS_1 \in \{0,1,2,3\ldots,9\}$ and $IS_2 \in \{0,1,2,3\ldots,9\}$ from the semantic image $SI \in \{0,1,2,3\ldots,255\}$ by using (3); Setting the threshold TH as 10; now, the intermediate shares IS_1 and IS_2 has the pixel values ranging between 0 and 9.

$$\begin{aligned} &IS_1{}^R \longleftarrow SI^R \; MOD \;\; TH \;\; IS_2{}^R \longleftarrow SI^R / TH \\ &IS_1{}^G \longleftarrow SI^G \; MOD \;\; TH \;\; IS_2{}^G \longleftarrow SI^G / TH \\ &IS_1{}^B \longleftarrow SI^B \; MOD \;\; TH \;\; IS_2{}^B \longleftarrow SI^B / TH \end{aligned} \tag{3}$$

Step 4: Intermediate Shares $IS_1 \in \{0,1,2,3\ldots,9\}$ and $IS_2 \in \{0,1,2,3\ldots,9\}$ can be embedded into cover images $CI_1 \in \{0,1,2,3\ldots,255\}$ and $CI_2 \in \{0,1,2,3\ldots,255\}$. To generate two shares $S_1 \in \{0,1,2,3\ldots,255\}$ and $S_2 \in \{0,1,2,3\ldots,255\}$. then, it will be delivered to the participants.

3.2. Revealing Phase

This section describes the proposed secret recovery scheme. After performing the sharing process for the n participants; each participant obtains one Stego-images. The proposed process of secret image recovery in the following steps,

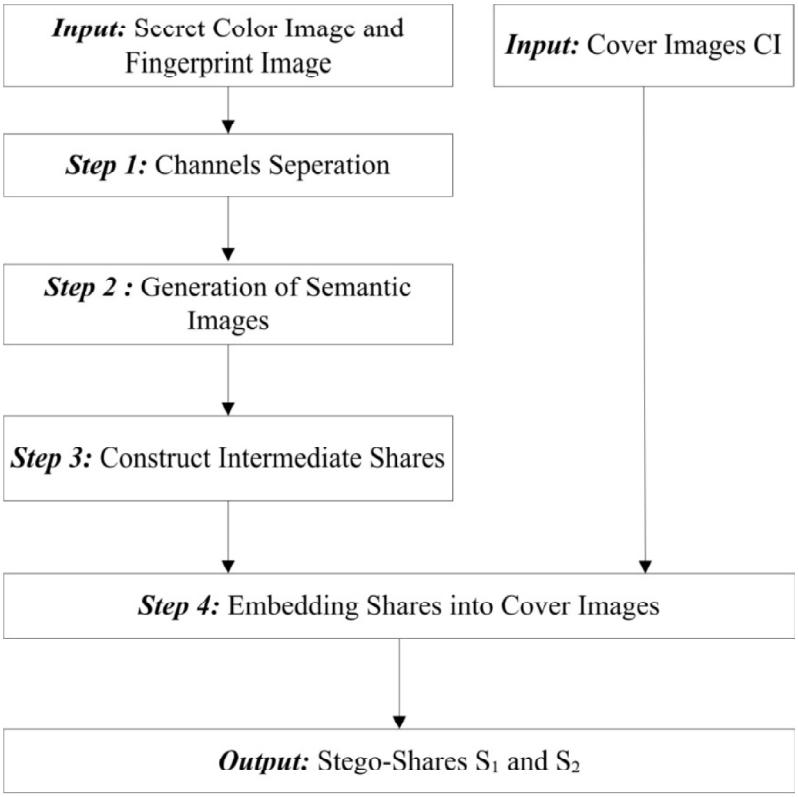


Figure 1: Flowchart of Sharing and Embedding phase

Input: The Random Number Generator (RNG) used to generate the integers $a_1, a_2 ...., a_n$ and a set of k stego-shares SH'_j.

Output: A report of failure of secret image reconstruction or recovered secret image I‘.

Step 1: Collect the stego images (4) $S_1 \in \{0,1,2,3\ldots,255\}$ and $S_2 \in \{0,1,2,3\ldots,255\}$.

$$\begin{aligned} {S_1}^R, {S_1}^G, {S_1}^B &\in \{0,1,2,3\ldots,255\} \\ {S_2}^R, {S_2}^G, {S_2}^B &\in \{0,1,2,3\ldots,255\} \end{aligned} \tag{4}$$

Step 2: Intermediate Shares $IS_1 \in \{0,1,2,3\ldots,9\}$ and $IS_2 \in \{0,1,2,3\ldots,9\}$ can be derived from share images (5).

$$\begin{aligned} {IS_1}^R, {IS_1}^G, {IS_1}^B &\in \{0,1,2,3\ldots,9\} \\ {IS_2}^R, {IS_2}^G, {IS_2}^B &\in \{0,1,2,3\ldots,9\} \end{aligned} \tag{5}$$

Step 3: To generate the reconstructed secret image I‘, digitally stacking $IS_2 \in \{0,1,2,3\ldots,9\}$ and $IS_2 \in \{0,1,2,3\ldots,9\}$ by using Random Number Generator (RNG) (6).

$$\begin{aligned} a &= {IS_1}^{i,j} + {IS_2}^{i,j} \\ r &= floor(rand(1) \times 9) \end{aligned}$$

$$I'^{i,j} = \begin{cases} ({IS_1}^{i,j} \times 10) + {IS_2}^{i,j} & if\ (a = 9) \,|\, (a = 18), \\ ({IS_1}^{i,j} \times 100) + ({IS_2}^{i,j} \times 10) + r & else, \end{cases} \tag{6}$$

Where;

i, j = varying from 0-255

a, r = varying integer values

Experimental Results

The proposed OVSS allows no limitation on the size of the secret images. The efficiency of the proposed method is tested in MATLAB 7.10 Tool and RIAtest tool [12]. Fingerprint (FT) image is obtained using U.are.U 4500 USB Fingerprint Reader [11] shown in Figure 2(b) [11]. OVSS scheme tested with one desktop computer, one Sony laptop with iPad for medical image communications.

(a) (b)

Figure 2: (a) 5079 -414 Electronic Stethoscope (b) U.are.U 4500 USB Fingerprint Reader

Proposed OVSS can be applied on various modalities like ECGHI images (Electrocardiography with Heart-tone Imaging), MRI (Magnetic Resonance Imaging), US (Ultrasonic), CT (Computed Tomography), Endoscopic and angiographic images. The heart sounds are recorded with the help of the 5079-430 Meditron Analyzer w/ECG using 5079-405(v) Elite Electronic Stethoscope [10] shown in Figure 2(a) and stored in the computer (PC). The output of the Meditron Analyzer ECG merges ECG signals with heart tones. It reveals the sounds present at the initial stages of functional and infectious diseases [10].

Figures 3(a), 3(b), 3(c), 3(d), 3(e), 3(f), 3(g) and 3(h) shows secret image ECGHI, cover images Baboon, Lena, Share1, Share2, reconstructed secret image ECGHI, Original Fingerprint image and Extracted Fingerprint image. Share images are looking different from the secret image; therefore, this method can escape from visual attack.

Table 1
Computational Analysis

Images	*Execution Time (Seconds)*
M1	8
M2	9
M3	7
M4	10
M5	7
M6	9

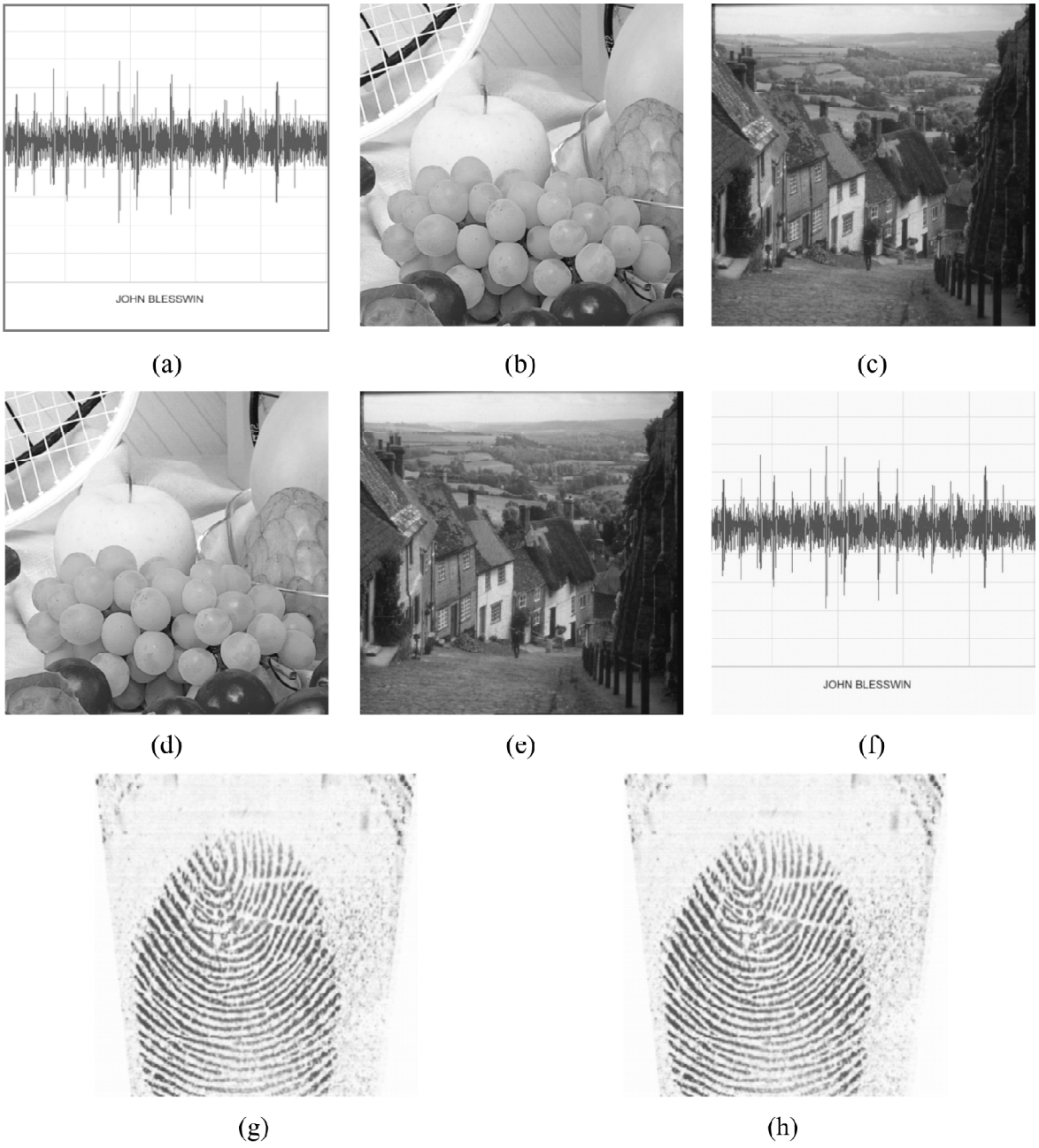


Figure 3: Experimental results

(a) Secret image, ECGHI (b) Cover image, Fruit (c) Cover image, Gold hill (d) Share1 (e) Share2, (f) Reconstructed image, ECGHI (g) Original Fingerprint image (h) Extracted Fingerprint image

The proposed work has been tested using real-time medical images those from SRM Hospital, Medical College and Research Center, Kattankulathur, India. The proposed work gave satisfied results and reduced errors. The work took 75 medical images such as ECG and CT images and the analyzed the computational time and quality measures for the images. Table 1 shows the time required to execute the algorithm on different images, and the result indicates that the method is less computational and efficient. The image quality measures such as Normalized Correlation (NC) and Peak Signal to Noise Ratio (PSNR) are evaluated between reconstructed medical images and original secret medical 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 logarithmic decibel is given by (7),

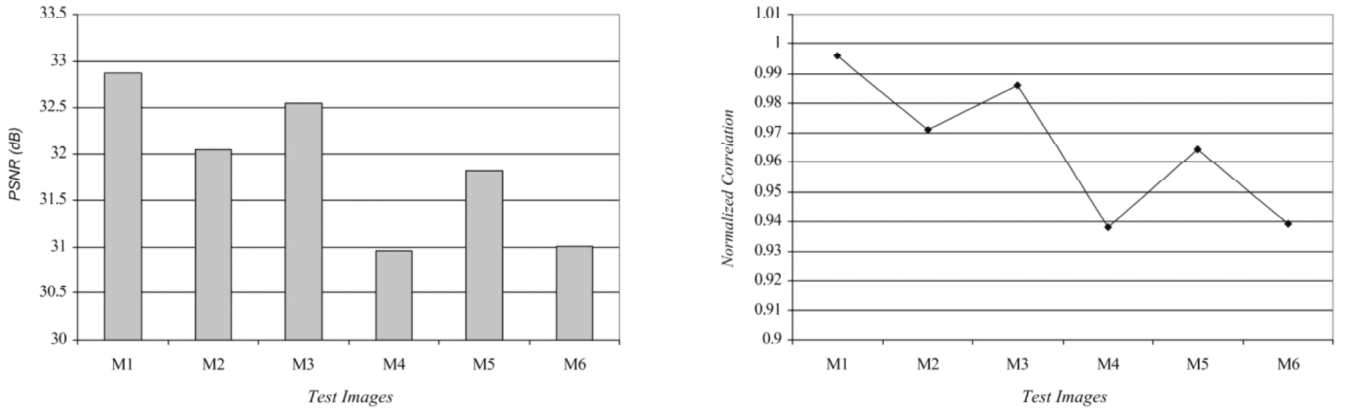
$$PSNR = \log \frac{(2^n - 1)^2}{MSE} \tag{7}$$

Normalized Correlation (NC): It measured the similarity representation between the original image and decrypted image (8),

$$NC = \frac{\Sigma_{i=1}^{M} \Sigma_{j=1}^{N} (I[i, j] I'[i, j])}{\Sigma_{i=1}^{M} \Sigma_{j=1}^{N} (I[i, j])^2} \tag{8}$$

Table 2
Results of various images

	Proposed scheme	
	NC	*PSNR*
M1	0.9962	32.88
M2	0.9711	32.05
M3	0.9862	32.55
M4	0.9380	30.96
M5	0.9641	31.82
M6	0.9395	31.01



(a) (b)

Figure 4: Graph representation of reconstructed image quality measures (a) *PSNR* (b*) NC*

The graph representation shows the various image quality measures in Figure 4. The PSNR values of the reconstructed secret images and the original images range from 30 to 32.88 dB. By seeing the obtained PSNR and NC values, reconstructed grayscale images can be presumed to be believable.

Table 2 represents the computed values for image quality evaluation for the reconstructed images. RIATest automated tool has been used to test the sufficiency of the proposed algorithm. The device has recorded actions, debugged the scripts, code completion and generated statistical reports. Fig. 5-7 shows the RIATest Tool images [12].

5. CONCLUSION

In this paper, novel optimal visual secret sharing scheme is proposed for color medical images. OVSS scheme preserves secret image by separating into multiple shares. Each share is visually undisturbed, and

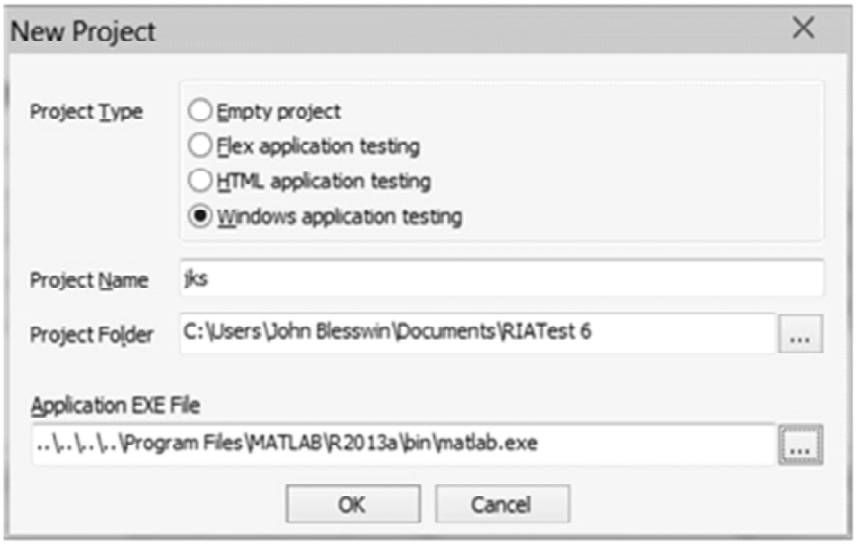


Figure 5: Creation of new project in RIATest Tool

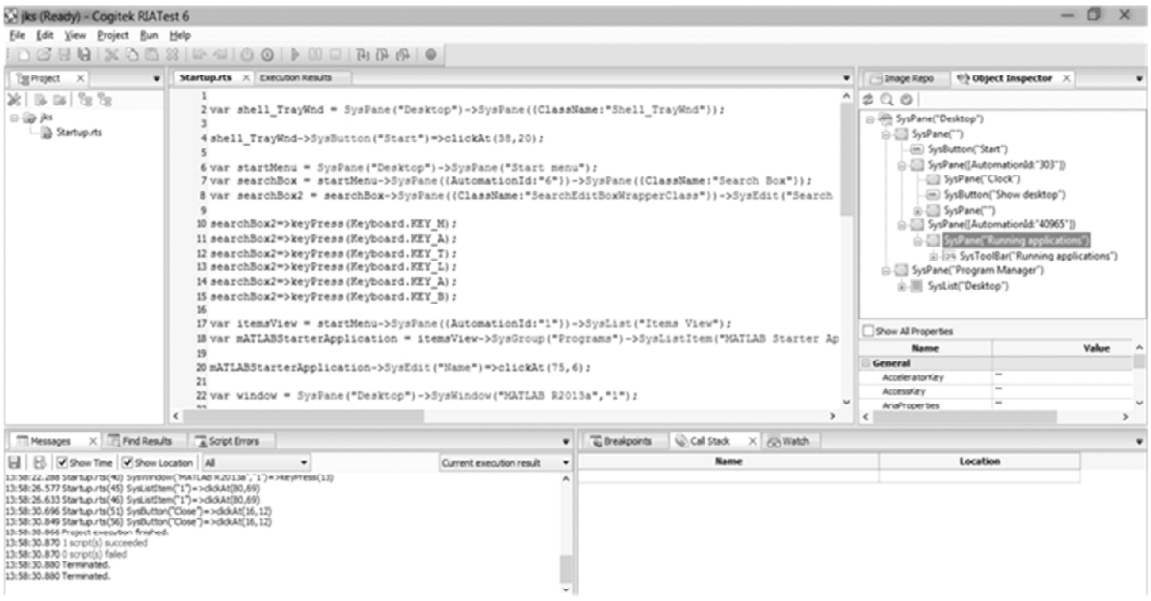


Figure 6: Running in RIATest Tool

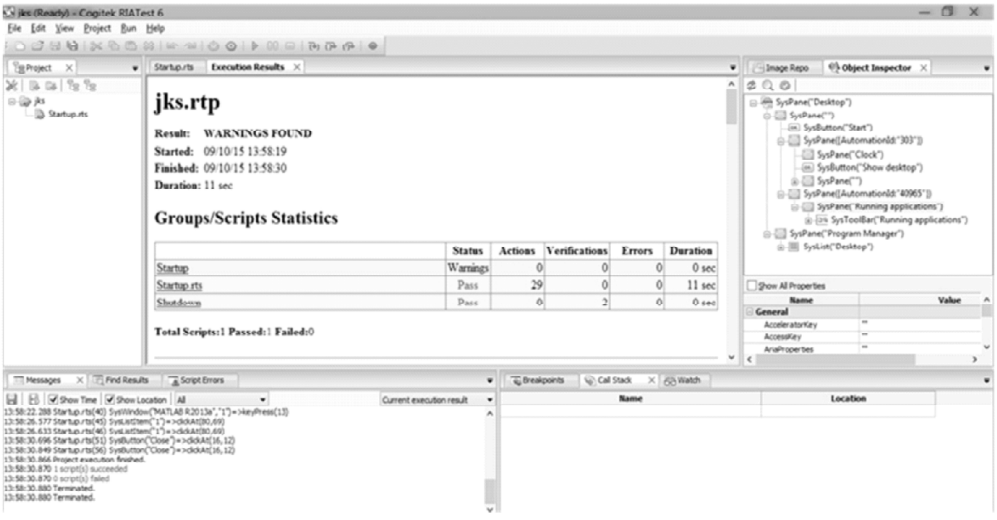


Figure 7: Generated Statistical Report Panel in RIATest Tool

its size is same as that of the original secret image. Moreover, the PSNR value of the reconstructed secret color image is larger than 35 dB, when no cheating occurs. There is a space for the development of OVSS for 3D medical images in the future.

ACKNOWLEDGMENT

The work is supported by the project "Development of Intelligent Secret Image Recovery Techniques using Visual Cryptography and Heuristic Optimization Techniques for Healthcare Applications" by University Grants Commission (UGC) for its financial assistance under major research projects in Engineering & Technology. We would also like to show our gratitude to Dr. Sundaram, Dean from SRM Hospital Medical College and Research Center, who provided facilities to test the proposed work in real time using images that greatly assisted the research.

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] Kai-Hui Lee, "Digital Image Sharing by Diverse Image Media" IEEE Transactions on Information Forensics and Security, Vol 9, pp. 88 - 98, 2014.

[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 Ng an 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 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), 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.

[10] *http://intl.welchallyn.com/images/products/fullsize/Blood%20Pressure%20Management/Electronic%20Stethoscope/Masterelite_5079430_product2_MC.jpg*

[11] *http://www.crossmatch.com/UareU4500Reader/*

[12] *www.cogitek.com/riatest.html*

[13] A. John Blesswin, Dr. P. Visalakshi, "Secret Sharing Approach on Electrocardiography with Heart Tone Images using Visual Cryptography for Secure Healthcare Communications", *Journal of Pure and Applied Microbiology*, Vol. 9(Spl. Edn. 1), 2015.