

Secret Sharing Approach on Electrocardiography with Heart tone Images Using Visual Cryptography for Secure Healthcare Communications

A. John Blesswin¹ and P. Visalakshi²

Department of Electronics and Communication Engineering,
PSG College of Technology, Coimbatore, India.

(Received: 16 February 2015; accepted: 10 April 2015)

In Medical imaging system, the patient's information plays an important role for tele-diagnosis, tele-health and tele-surgery. Medical image communication has become popular in public networks with the enormous growth in Internet technologies. Medical image verification is vital to ensure the privacy of the patient's information. The conventional cryptography framework encrypts the secret medical information in a more complex, time-consuming and tedious process. A novel scheme called a Verifiable Secret Image Sharing (VSIS) scheme is proposed which is suitable for medical color image communications. The proposed method converts the medical color image into semantic image by using Dynamic Error Reduction (DER) technique for reducing the encoding complexity. The semantic image is encrypted into n shares and hidden into the cover images called stego-shares, to avoid malicious attacks. In the revealing side, the secret image is reconstructed using the shares, having no correlation with cover images. Based on the extracted token image in the revealing phase, the proposed VSIS scheme provides a good solution for improving the reliability, by the verification of collected shares and thereby identifying the cheating party. The experiment ensures the security, reliability and quality of the proposed scheme..

Key words: Medical image communication, Secret sharing, Security, Shares, Visual Cryptography.

Information Security (IS) is one of the important issues of Medical Communication Systems (MCS). Medical image security is a key issue when patient's information like medical images is communicated through public networks to the Health Centers for tele-health applications. Conventional security methods are not suitable for protecting medical images during data transmission. Image security applications have high priority for encoding the secret information in electronic media¹⁴. To deal with the security issues, the Health Insurance Portability and

Accountability Act [8] (HIPAA) called for medical contributors to implement the procedures for the protection of medical information¹⁵. Visual Cryptography (VC) is a unique method to generate random and natural shares, for sharing secret images. Many secret sharing schemes have been developed using adopted stacking approaches¹⁻⁴. In 1994, Naor and Shamir¹ used visual secret sharing method to generate two shares by the combination of black and white pixels based on the secret image. In 1997, first color visual sharing scheme was introduced by Verheul and Tilborg², where each color image is separated into red, green and blue channels, where pixel expansion is $c \times 3$. The pixel expansion is minimized into $c \times 2$ by Yang and Laih³. Chang *et al.*,⁴ first formed a color index table to produce the two camouflage shadows from

* To whom all correspondence should be addressed.
E-mail: wjohnbless@gmail.com

the secret color image. Jin *et al.*,⁵ proposed the VC scheme; binary shares are produced from the color pixels by mono encryption and multiple decryption methods. In the adopted stacking approaches⁴⁻⁷, the process is good, but leads to pixel expansion and high computational complexity.

Related Work

Dynamic Error Reduction (DER)

A Dynamic Error Reduction (DER) process generates a Semantic Image (SI) from a single level image I, this simple and attractive design decreases the errors and reduces the encoding complexity. A flowchart of dynamic error reduction is shown in Fig. 1. This section describes the new Semantic Error Filter (SEF) strategy, which helps to get the coefficients in an integer form. The semantic image is generated from an error reduction strategy with the help of an error filter. The SEF consists of kernel weights. The kernel weights are $I(x,y)/100$, $(I(x,y)/10) \bmod (10)$ and $I(x,y) \bmod 10$. Error values are determined based on the secret pixels. Semantic image has clusters of same pixel values, when compared to the original secret image. Pixels with the similar values cluster together in a continuous region. Hence, it will result in no loss of image luminance¹⁸.

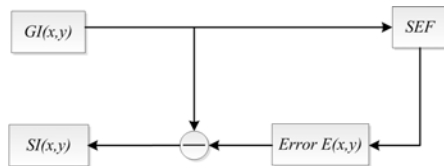


Fig. 1. Flowchart of Dynamic Error Diffusion

MATERIAL AND METHODS

The proposed Verifiable Secret Image Sharing Scheme (VSIS) methodology ensures robust visual secret sharing with reduced computational complexity. First, the secret image is processed by the dynamic error reduction technique. Then, the intermediate shares IS_1 and IS_2 are constructed, which is embedded into natural cover images CI_1 and CI_2 .

Share Image Generation

Dynamic Error Reduction (DER) process generates a Semantic Image (SI) from a single level image I, this simple and attractive design decreases the errors and reduces the encoding complexity. This section describes the procedure to generate

the Token Image (TI), and the shares S_1 and S_2 from the secret image. Secret color image is decomposed into Red, Green and Blue (RGB) sub-images. From these sub-images, the stego-shares S_1 and S_2 are generated. The share image generation procedure is illustrated as follows:

Input

Original color secret image I with $W \times H$ pixels and two cover images (CI_1 and CI_2).

Output: Two stego-shares (S_1 and S_2).

Step 1) Consider $W \times H$ secret medical color image, denoted as I and natural color image as the cover images CI_1 and CI_2 (1); for each position $(i, j) \in \{(i, j) | 1 \leq i \leq W, 1 \leq j \leq H\}$ of I, repeat Steps 2-4.

$$\begin{aligned}
 [I] &\rightarrow I^R, I^G, I^B \\
 [CI_1] &\rightarrow CI_1^R, CI_1^G, CI_1^B \\
 [CI_2] &\rightarrow CI_2^R, CI_2^G, CI_2^B
 \end{aligned} \dots(1)$$

Step 2

Generate SI, by applying the dynamic error reduction technique on the secret color image (2); obviously, the width and height of SI are W and H. Moreover, each pixel in SI contains only 8 bit. The token image is a half-sampled image of I, which is created by using the discrete wavelet transform technique. In this step, convert a secret image to a Halftone Image (HI) with the help of error diffusion method¹⁶ and perform single-level decomposition on HI using db4 wavelet type. TI is created by using the coefficient matrices of the level-one approximation (cA1).

$$\begin{aligned}
 I^R, I^G, I^B &\rightarrow DER \rightarrow SI^R, SI^G, SI^B \\
 SI^R, SI^G, SI^B &\in \{0,1,\dots,243\}
 \end{aligned} \dots(2)$$

Step 3

Construct the intermediate shares, denoted as $IS_1 \in \{0,1,2,3,\dots,9\}$ and $IS_2 \in \{0,1,2,3,\dots,9\}$ from semantic image $SI \in \{0,1,\dots,243\}$ by dynamic error reduction. IS_1 and IS_2 have the pixel values ranging between 0 and 9.

$IS_1(i, j)$ $a_7a_6a_5a_4a_3a_2a_1a_0$	$IS_2(i, j)$ $b_7b_6b_5b_4b_3b_2b_1b_0$
$CI_1(i, j)$ $c_7c_6c_5c_4c_3c_2c_1c_0$	$CI_2(i, j)$ $d_7d_6d_5d_4d_3d_2d_1d_0$
$S_1(i, j)$ $e_7e_6e_5e_4e_3e_2e_1e_0$	$S_2(i, j)$ $d_7d_6d_5d_4b_3b_2b_1b_0$

Fig. 2. The ij^{th} pixel of IS_1 is embedded into CI_1 ; the ij^{th} pixel of IS_2 is embedded into CI_2

Step 4

IS_1 and IS_2 can be embedded into cover images CI_1 and CI_2 respectively. Four bits are taken from IS_1 and IS_2 and embedded by using LSB¹¹ embedding procedure on CI_1 and CI_2 . It provides high encoding capability and also assures that the two shares can be completely restored after stacked from S_1 and S_2 . The shares are delivered to the participants. For simplicity, assume that $IS_1(i,j)$ is the ij^{th} pixel that can be embedded into $CI_1(i,j)$ and $IS_2(i,j)$ is the ij^{th} pixel that can be embedded into $CI_2(i,j)$ as shown in Fig. 2.

Here, the binary representations of the pixels $IS_1(i, j), IS_2(i, j), CI_1(i, j)$ and $CI_2(i, j)$ are $a_0, a_1 \dots a_7, b_0, b_1 \dots b_7, c_0, c_1 \dots c_7$ and $d_0, d_1 \dots d_7$ respectively. Consider $a_3a_2a_1a_0$ and $b_3b_2b_1b_0$ to be the secret information bits. The last four LSBs of $CI_1(i, j)$ are replaced by $a_3a_2a_1a_0$. Similarly in the pixel $CI_2(i, j)$, the last four LSBs [8] can be replaced by $b_3b_2b_1b_0$ as shown in Fig. 2. Since only the LSBs of the pixels are modified, there is not much degradation in the quality of the image. In the proposed method, participants of the valid shares can reveal the secret image. However, participants of the invalid shares, get no clue about the secret information.

The cover images are used to improve the security of the VSIS scheme. Intermediate shares can be covered by natural color images [13]. No secret data is available to attacker, regarding the original secret information as long as the k valid shares are not collected during the revealing phase [12]. In addition, one more assumption is required in the proposed VSIS scheme. The sender must register with the issued token image with the Trusted Third Party (TTP) before sending the shares to participants during the share image generation phase. TTP verifies the token image and checks whether the token image is the same as the sampling of the secret image. If it is same, the TTP accepts the sender's request; otherwise, TTP rejects the sender's request. This assumption ensures the reliability of the shares.

Revealing Phase

This section describes the secret image recovery scheme. It is known that after performing the sharing process with the n participants, each

participant obtains one stego-image. The process of secret image recovery is done using the following steps,

Input: Stego-shares S_1 and S_2

Output: Recovered secret image or a report of failure

Step 1

Collect the share images (3) $S_1' \in \{0,1,\dots,243\}$

and $S_2' \in \{0,1,\dots,243\}$.

$$\begin{aligned} S_1^{R'}, S_1^{G'}, S_1^{B'} &\in \{0,1,\dots,243\} \\ S_2^{R'}, S_2^{G'}, S_2^{B'} &\in \{0,1,\dots,243\} \end{aligned} \quad \dots(3)$$

Step 2

$IS_1' \in \{0,1,\dots,9\}$ and $IS_2' \in \{0,1,\dots,9\}$ can be derived from share images (4). Here, the binary representations of the pixels $S_1(i, j), S_2(i, j), E_1(i, j)$ and $E_2(i, j)$ are $a_0, a_1 \dots a_7, b_0, b_1 \dots b_7, c_0, c_1 \dots c_7$ and $d_0, d_1 \dots d_7$.

Consider E_1 and E_2 are empty and filled with zeros, replace the last four bits of E_1 by $a_3a_2a_1a_0$. Similarly, replace the last four bits of E_2 as shown in Fig. 3.

$$\begin{aligned} IS_1^{R'}, IS_1^{G'}, IS_1^{B'} &\in \{0,1,\dots,9\} \\ IS_2^{R'}, IS_2^{G'}, IS_2^{B'} &\in \{0,1,\dots,9\} \end{aligned} \quad \dots(4)$$

$S_1(i, j)$ $a_7a_6a_5a_4a_3a_2a_1a_0$	$S_2(i, j)$ $b_7b_6b_5b_4b_3b_2b_1b_0$
$E_1(i, j)$ $c_7c_6c_5c_4c_3c_2c_1c_0$	$E_2(i, j)$ $d_7d_6d_5d_4d_3d_2d_1d_0$
$IS_1(i, j)$ $c_7c_6c_5c_4a_3a_2a_1a_0$	$IS_2(i, j)$ $d_7d_6d_5d_4b_3b_2b_1b_0$

Fig. 3. The ij^{th} pixel of IS_1 is extracted from S_1 and the ij^{th} pixel of IS_2 is extracted from S_2 .

Step 3

To generate the reconstructed secret image I' , stack $IS_1^{k'} \in \{0,1,\dots,9\}$ and $IS_2^{k'} \in \{0,1,\dots,9\}$ by using (5). Let Threshold TH be 9.

$$\begin{aligned} a &= IS_1^{k'}(i, j) + IS_2^{k'}(i, j) \\ IS_3^k(i, j) &= \begin{cases} TH - a & \text{if } (a < TH), \\ 1 & \text{if } (a \geq TH), \end{cases} \quad \dots(5) \end{aligned}$$

$$I^{k'}(i, j) = (IS_1^k(i, j) \times 100) + (IS_2^k(i, j) \times 10) + (IS_3^k(i, j))$$

Where

$$(i, j) \in \{(i, j) | 1 \leq i \leq W, 1 \leq j \leq H\}$$

a = varying integer values

Finally, Step 3 is applied to each sub-image separately. Finally, the reconstructed secret image is created by concatenating the three reconstructed sub-images together.

Verification Phase

This phase checks the reliability of the reconstructed image from the set of collected shares; it also helps to find the fake share from the set of collected shares.

Step 1

Given reconstructed secret image (I'), perform the sampling by discrete wavelet transform to retrieve the new reconstructed token image (TI'). TI' is used to serve the purpose of reliability.

Step 2

This step checks whether any cheating occurs by using the token image TI, which is generated from Step 2 in the share image generation phase. TI' depends on the shares S₁ and S₂, if there is no tampering or cheating, the shares S₁' and S₂' in the revealing phase are the same as the shares S₁ and S₂ in the share image generation phase. That is, TI' is the same as token image TI.

Obviously, TI' and TI are the same because the proposed method does not affect the token image. Consider d to be the difference between TI and TI', $d = TI - TI'$. If the value of d is equal to zero, I' is reconstructed completely. Otherwise, senders and participants come under mistrust, when d is not equal to zero value.

RESULTS AND DISCUSSION

Experimental results satisfy three objectives: high quality reconstruction, no pixel expansion and reliable verification of the reconstructed secret image. The proposed VSIS has no limitation on the size of the secret images. The set of test images shown in Figure 4 illustrates that VSIS can perform well on color images. The efficiency of the proposed method is tested using MATLAB tool. Computational cost of VSIS scheme depends on two operations: error reduction and bitwise operations. It does not have much effect on complexity of the proposed scheme.

Table 1. Computational complexity of VSIS Scheme with color images

Color Image	Execution time
ECGHI 1	45s
ECGHI 2	47s
CT 1 Brain image	42s
CT 1 Chest image	44s

The simulation results of the execution time of the proposed scheme are shown in Table 1. Proposed VSIS 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 Meditron Analyzer ECG using Elite Electronic Stethoscope [17] and stored in the personal 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 diseases¹⁷.

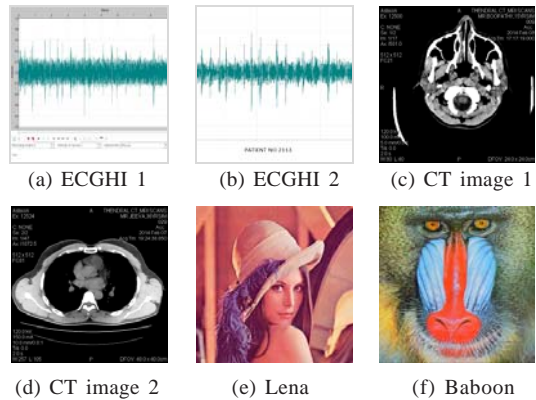


Fig. 4. Eight 512x512 grayscale images

The image quality measures such as Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM) and Normalized Correlation (NC) are evaluated between reconstructed image and original secret image using following equations. 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 as given by⁶,

$$PSNR = \log \frac{(2^n - 1)^2}{MSE} \dots(6)$$

Structural Similarity Index (SSIM): It measures the similarity of two images, based on an initial uncompressed or distortion-free image⁷.

$$SSIM(x, y) = \frac{2 \times m_1(P) \times m_2(P) + C_1}{m_1(P)^2 + m_2(P)^2 + C_1} \times \frac{2 \times c(P) + C_2}{s_1(P)^2 + s_2(P)^2 + C_2} \dots(7)$$

Table 2. Values of PSNR, SSIM, NC

Color Image	PSNR	SSIM	NC
ECGHI 1	37.2 dB	0.970	0.969
ECGHI 2	37.4 dB	0.975	0.995
CT 1 Brain image	36.7 dB	0.956	0.956
CT 1 Chest image	36.2 dB	0.943	0.942

Where $m_1(P)$ and $m_2(P)$ are mean values, $s_1(P)$ and $s_2(P)$ are standard deviations of seq_1 and seq_2 , $c(P)$ is the covariance between seq_1 and seq_2 , computed over the same window, $C_1 = (K_1 * L)^2$: regularization constants, $C_2 = (K_2 * L)^2$, K_1, K_2 : regularization parameters, $L=255$ and the default window is a Gaussian window with standard deviation 1.5 along both the X and the Y axis. Table 2 represents the computed values for image quality evaluation for the reconstructed images. Normalized Correlation (NC): It measures the similarity representation of the original image and decrypted image (8).

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

Table 3. Image quality of the reconstructed secret image, extracted token image error and reliability conclusion when no cheating is detected

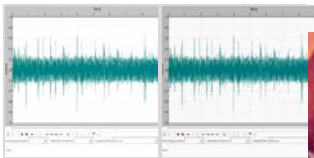
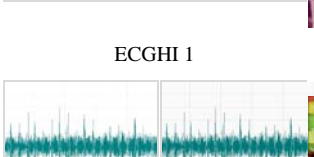




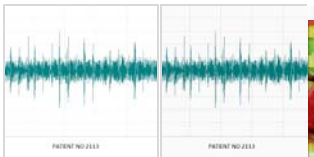
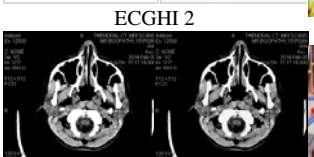




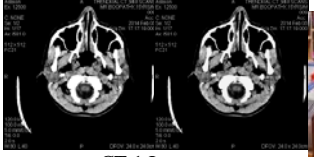
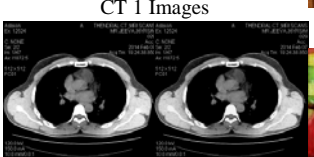

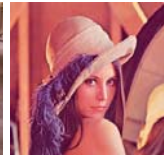


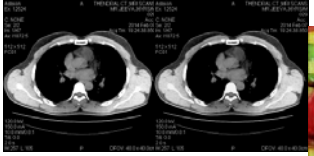
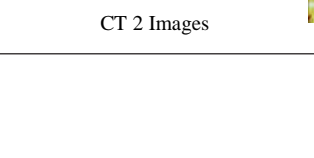




Original color image	Reconstructed color image	Share1	Share2	Original token image	Extracted token image	Reliability
						Sure
ECGHI 1				MSE=0		
						Sure
ECGHI 2				MSE=0		
						Sure
CT 1 Images				MSE=0		
						Sure
CT 2 Images				MSE=0		

Table 4. Reconstructed secret image quality, extracted token image and the extracted result when cheating occurs

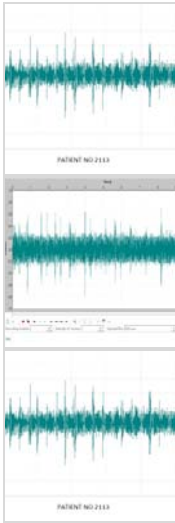
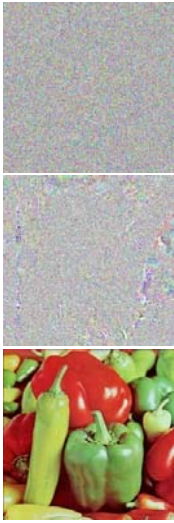
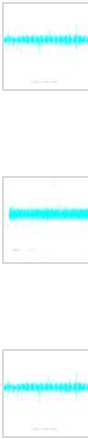

Original color image	Reconstructed color image	Original token image	Extracted token image	Cheating type	Reliability
				(1)	Not Sure
				(2)	Not Sure
				(3)	Not Sure

Table 5. Comparison of the proposed scheme and other VC schemes

Criteria	[9]	[10]	[11]	Proposed scheme
(A)	$n \geq 2$	$n \geq 2$	$n \geq 2$	$n = 2$
(B)	$MSE > 0$	$MSE > 0$	$MSE > 0$	$MSE = 0$
(C)	Uses difficult base matrices	Uses Complex Genetic algorithm	Uses embedded authentication code	Uses extracted TI to verify the reconstructed image
(D)	$(2^n + n + 1) \times N$	$n \times N$	$N \times 1.15$	N
(E)	High	High	High	Relative Low

Where $I(i, j)$ is the original image and $I'(i, j)$ is the decrypted image, M is the height of the image and N is the width of the image.

The experiments were performed under two circumstances. The first is that, no cheating or tampering is caused during communications. The reconstructed secret image quality and extracted token image are shown in Table 3. The second circumstance, shown in Table 4, assumes that some cheating has occurred in shares by dishonest participants. To evaluate the reliability of the reconstructed secret image, the reliability factor uses two values: “Sure” and “Not sure”. If the MSE value of TI and TI' is zero, the factor is “Sure” and vice versa. To demonstrate the

verification ability of the proposed scheme, the shares have been altered by dishonest participants as shown in Table 5. Three scenarios of cheating are considered as follows:

1. “ECGHI 1” is the original secret image and corresponding TI is the token image. The first share is replaced by fake share.
2. “ECGHI 2” is the original secret image and corresponding TI is the token image. The first share is not changed, but the second share is replaced by a fake share.
3. “ECGHI 2” is the original secret image and corresponding TI is the token image. The first share is replaced by a fake share, which is the second share when “Pepper” is the

original secret image.

Discussion and comparisons

To demonstrate the advantage of the proposed scheme, the comparison is shown in Table 5. Five evaluation criteria are used to compare the proposed scheme with other VC schemes: number of shares (A), MSE value between secret image and reconstructed secret image (B), cheating prevention method (C), shares size (D) and computational complexity (E).

1. Number of shares (A): The value n is the total number of shares generated by the share construction phase in the proposed scheme.
2. MSE value between secret image and reconstructed secret image (B): This value is used to calculate the similarity of two images.
3. Cheating prevention method (C): It specifies the idea of the cheating prevention mechanism of the VC scheme.
4. Shares size (D): It compares the size of the secret image and the shares.
5. Computational complexity (E): It specifies the execution time of the operations performed which is given by time complexity $O(n)$.

CONCLUSION

In this paper, novel verifying secret image sharing scheme is proposed for medical color images. VSIS scheme preserves secret image by separating into multiple shares. It also checks the reconstructed secret medical image and unveils the cheating type, when some of the collected share is replaced by fake share. Each share is visually undisturbed and 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 development of VSIS for 3D images in the future.

ACKNOWLEDGEMENTS

The work is supported with the project of "Design and development of intelligent secret image recovery techniques" by University Grants

Commission (UGC), New Delhi for its financial assistance under major research projects in Engineering & Technology on January 2013.

REFERENCES

1. M. Naor & A. Shamir, "Visual Cryptography", Eurocrypt, *Lecture Notes in Computer Science*, 1995; **950**: 1-12.
2. E. Verheul & H. V. Tilborg, "Constructions and Properties of K out of N Visual Secret Sharing Schemes", *Designs, Codes and Cryptography*, 1997; **11**: 179-196.
3. C. Yang & C. Laih, "New Colored Visual Secret Sharing Schemes, Designs", *Codes and cryptography*, 2000; 325-335.
4. C Chang, C Tsai, & T Chen, "A New Scheme For Sharing Secret Color Images In Computer Network", *International Conference on Parallel and Distributed Systems*, 2000; 21-27.
5. Jin D, Yan W & Kankanhalli, "Progressive color visual cryptography", *J. Electron. Imaging*, 2005; 14.
6. Shyong Jian Shyu, "Visual Secret Sharing Scheme for Color Images", *Pattern Recognition Letters*, 2006; **39**: 866-880.
7. C.-C. Chang, C.-C. Lin, C.-H. Lin, & Y.-H. Chen, "A Novel Secret Image Sharing Scheme in Color Images Using Small Shadow Images", *Information Sciences*, 2008; **178**: 2433-2447.
8. C.-K. Chan & L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, 2004; **37**: 469-474.
9. R. D. Prisco & A.D. Santis, "Cheating immune (2, n)-threshold visual secret sharing", *Proceedings of Security and Cryptography for Networks*, 2006; **4116**: 216-228.
10. S. Tsai, T.H. Chen & G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images", *Pattern Recognition*, 2007; **40**: 2356-2366.
11. C.N. Yang, T.S. Chen, K.H. Yu & C.C. Wang, "Improvements of image sharing with steganography and authentication", *Journal of Systems and Software*, 2004; **73**: 405-414.
12. Li, Ling Chen & Shuenn-Shyang Wang, *Visual Cryptography for meaningful shares*, Thesis for master science, Institute of communication engineering, Tatung University, 2007.
13. Kai-Hui Lee, "Digital Image Sharing by Diverse Image Media", *IEEE Transactions on Information Forensics and Security*, 2014; **9**: 88-98.
14. J. Fridrich, "Steganography in Digital Media: Principles, Algorithms and Applications", *IEEE*

- Signal Processing Magazine, 2011; **28**: 142-144.
15. "Health Insurance Portability and Accountability Act (HIPAA) and Its Impact on IT Security," Regulatory Compliance Series 3 of 6, Apani Networks White Paper Compliance Series. May 12, 2005. <http://www.apani.com>.
 16. J. B. Feng, I. C. Lin, & Y. P. Chu, "Halftone image resampling by interpolation and error-diffusion", International Conference on Ubiquitous Information Management and Communication, 2008.
 17. http://intl.welchallyn.com/documents/Blood%20Pressure%20Management/Electronic%20Stethoscope/user_manual_stet_complete.pdf
- A. John Blesswin & P. Visalakshi, "Multi-Secret Semantic Visual Cryptographic Protocol for Securing Image Communications", *Asian Journal of Inf. Technology*, 2014; **13**: 506-512.