New Fool Proof Examination System through Color Visual Cryptography and Signature Authentication

Mohamed Fathimal[1] and Arockia Jansirani[2]
[1]Department of Computer Science and Engineering, SRM Institute of Science and Technology, India
[2]Department of Computer Science and Engineering, Manonmaniam Sundaranar University, India

Abstract: *There have been widespread allegations about the question papers leakage for a number of subjects in the recently held Secondary School Leaving Certificate examinations. The leakage is due to the practice of using printed question papers. Such incidents and subsequent cancellation of examinations are happening frequently. This creates political and social embarrassment and causes loss of money and time. This paper proposes a new system of foolproof examination by tamperproof e-question paper preparation and secure transmission using secret sharing scheme. The application is perfectly secure because the proposed method automatically embeds the corresponding institute seal in the form of the key. As a result, it is easy to trace out the source culprit for the leakage of question papers. This scheme has reduced reconstruction time because the reconstruction process involves only Exclusive-OR (XOR) operation apart from authentication. The proposed method recovers the original secret image without any loss. The existing visual cryptographic scheme recovers half-toned secret image with average Peak Signal-to-Noise Ratio (PSNR) value 24dB. Further, it shall be stated that the proposed method with authentication recovers the image with 64.7dB PSNR value, which is greater than that of the existing method. In addition, this method does not suffer from pixel Expansion.*

Keywords: *Visual cryptography, secret sharing scheme, examination system, information security, authentication.*

Revived August 20, 2014; accepted March 9, 2016

1. Introduction

The backbone of a nation is education and is a vital indicator in calculating human development. Nowadays, the ability of an individual is assessed through examinations and people are much conscious and concerned about their education. Two major problems faced by the current education system are ensuring the conduct of foolproof examinations and providing tamper proof certificates. Currently various competitive examinations, regular school and university examinations are using printed question papers.Students those get the leaked question papers pass their exams and get jobs in important sectors where talented students face real hardship of exams and scoring up to their splendor. Therefore, the reliability and security of question papers is of paramount importance to ensure educational and social justice.

To achieve secure transmission of data, usually the data is concealed using symmetric or asymmetric key cryptography, which involves high computation and cost effective in encryption and decryption process. The main aim of this paper is to overcome this drawback by employing secret sharing scheme for this application. The main concept of the original Visual Secret Sharing (VSS) scheme is to encrypt a secret image into number of meaningless share images. It cannot leak any information of the shared seret by combination of the share images except for all of the shares.

This paper proposes a security system for tamperproof e-question paper sharing scheme using simple arithmetic operations. The secret sharing scheme has two categories–visual cryptography scheme and polynomial based secret sharing scheme. Visual cryptography introduced by Naor and Shamir [12] in 1994, is a type of secret sharing techniques for bi-level images in which decryption is performed by superimposing the shares without any computation involved. Existing color visual cryptography methods did not generate good quality reconstructed version of the original document due to half-toning effect. The polynomial based secret sharing scheme introduced by Shamir involves high computational complexity. However, the proposed tamperproof e-question paper system results in better visual quality of the reconstructed image without any pixel expansion and reduced computational complexity.

2. Literature Survey

Verheul and Tilborg [18] were the first to consider color visual cryptography, where the pixels in the secret image are taken from a given set of colors. Their model assumes that, when superimposing pixels of different colors, one sees a special black color. For a colored visual cryptography scheme with *c* colors, the pixel expansion m is *c*3*.Hence in this model, there is an additional loss of resolution by a factor of *c*.

Yang and Laih [20] reduced the pixel expansion to *c*2* of Verheul and Tilborg [18]. However, both schemes generated meaningless shares only. Shyu [13] advised a more efficient colored visual secret sharing scheme with pixel expansion of the order of log2 c*m where m is the pixel expansion of the exploited binary scheme. In most color visual cryptography schemes, when two pixels of the same color are superimposed, the resultant pixel gets darker. Cimato *et al*. [2] examine this color darkening by proposing a scheme, which has to guarantee that the reconstructed secret pixel has the exact same color as the original. Kang *et al*. [10] proposed a k out of N Color Extended Visual Cryptography scheme using Visual Information Pixel (VIP) synchronization and error diffusion [4]. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels Error diffusion is used to construct the shares such that the noise introduced by the preset pixels are diffused away to neighbors when encrypted shares are generated. This scheme could recognize the colorful secret messages having even low contrast and produces meaningful color shares with high visual quality. However, this scheme also suffers from the problem of Pixel Expansion. Monoth [11] presented three different methods to improve the contrast of visual cryptography schemes- Additional Basis Matrix, Perfect Reconstruction of White Pixels and Perfect Reconstruction of White Pixels with Additional Basis Matrix and applied for tamperproof preparation and transmission of online question papers and fingerprint images.

Thien and Lin [15] adopted the Shamir-Lagrange technique to share image secretly. Many researchers have proposed functional secret image sharing schemes based on sharing as meaningless shares (Fathimal [3]; Fathimal [5]), among host images (Guo *et al*. [9]; Wu *et al*. [19]; Ulutas *et al*. [17]) and sharing with authentication (Yang *et al*. [21]; Tu *et al*. [16]; Fathimal [6, 7, 8]). Chen *et al*. [1] developed the secret image sharing method based on the Lagrange's interpolating polynomial. The n shadow images of the secret image were made by compressing, substitute, encoding and disassemble to the secret image, each shadow image is hidden in an ordinary image so as not to attract an attacker's attention.

3. Block Based Secret Image Sharing Scheme

This section clearly describes the proposed encryption and decryption algorithm.

Algorithm 1: Encryption Module

*Input: Secret image I of size m*n*
Number of shares N
Key Image of any size
*Output: N meaningful shares of size m*n.*
Step 1: Key Generation Module
*Expand key to the size equal to the secret image size m*n.*
Step 2: Normalized Matrix Computation
The adaptively normalized matrix a(i) is computed by using the formula,

$$a(i)=\begin{cases} I_p/n+(i-1) & \text{if } i<n \\ I_p-\sum_{k=0}^{n-1} a(k) & \text{if } i=n \end{cases}$$

where $i=1,2,3,..n; n=\log_2 N$.
Step 3: Source Matrix Formation
The source matrix s(i) is derived from a(i)

$$s(i)=\begin{cases} 2^{8-j}-a(i) & \text{if } i \text{ is odd number} \\ a(i) & \text{if } i \text{ is an even number} \end{cases}$$

where $j=i/2+1$.
Step 4: Share Generation
Generate N numbers of shares $S_1, S_2, S3...S_N$ *of size m*n using*

$$S_i = \text{bitxor}(X, Y)$$

where

$$X=\begin{cases} key & \text{if } i=1 \\ s(i-1) & \text{if } i<=n+1 \\ Y(i-1) & \text{if } i>n+1 \end{cases}$$

$$Y=\begin{cases} s(i) & \text{if } i<=n \\ S_1 & \text{if } i=n+1 \\ S_{i-3} & \text{if } i>n+1 \\ \text{bitxor}(I_p, key) & \text{if } i=N \end{cases}$$

Algorithm 2: Decryption Module

In the receiver side, the following one-step formula reconstructs the secret image
Secret Image = $S_1 XOR S_2 XOR S_3 XOR ... S_N$.

4. Examination Automation System

The proposed examination automation system has three Modules.

4.1. Question Paper Preparation Module

This module prepares the question paper in image format (.jpg, .bmp, .gif, .png, .tiff) is broken into two pieces using block based secret image sharing algorithm where each piece seen individually will have no information about the question logo of the university. This module then distributes the shares to two trusted parties.

More than one question papers for each subject has been prepared and saved in two shares.

Algorithm 3: Question Paper Preparation Module

*Input: 1.Question Paper Image of size m*n*
2. Key Image of any size k1
*Output: 2 Shares of size m*n*
Step 1:
Apply block based Encryption algorithm to generate shares using key k1.
Step 2:
Hand over the shares to trusted parties.

4.2. Question Paper Distribution Module

This module randomly selects one question paper, their shares are decrypted, and recovered question paper is again subject to block based secret image sharing algorithm using different keys for generating shares to examiners. This module then embeds the signatures of the examiners in two shares using Least Significant Bit (LSB) Algorithm i.e., it embeds the signature of the controller of examination center's (Internal Examiner) in one share and distributed to the external representative. Similarly, it embeds the external representative's signature in another share and distributed to the controller of examination centre.

Algorithm 4:Question Paper Distribution Module

*Input: 1. 2 shares of size m*n*
2 .key image k2 of any size
Step 1:
Apply decryption Algorithm to regenerate the question paper.
Step 2:
Apply block based Encryption algorithm to produce shares using key k2.
Step 3:
Embed Signature of External Examiner in share 1.
Step 4:
Embed Signature of Internal Examiner in share 2
Step 5:
Distribute the share1 to Internal Examiner and Share 2 to External Examiner.

4.3. Question Paper Reconstruction Module

This module delivers question papers with authorized access just 30 minutes before exams start. This module collects the shares and signatures of controller of examination center and external representative. Then it compares the signatures with the signatures extracted from the shares to ensure authenticity. If the shares are equal, then the shares are superimposed using decryption algorithm (xor operation) to recover the question paper. If the signatures are not equal, this method will give error message about unauthenticated access. Thus, this module helps to provide authenticated access to reconstruct the question paper.

Algorithm 5: Question Paper Reconstruction Module

*Input: 1. 2 shares of size m*n.*
2. Signature of External and Internal Examiner
*Output: Recovered Question paper Image of size m*n.*
Step 1:
Extract signatures from shares.
Step 2:
Match the input signatures with the signature extracted from shares.
Step 3:
If both are equal, XOR the shares and the question paper will be recovered.
Step 4:
It both signatures are not equal, unauthenticated access error message will be displayed.

5. Performance Metrics

5.1. Peak Signal to Noise Ratio (PSNR)

The simplest and most widely used pixel wise error based measures are Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The MSE is the squared intensity differences between the reference and the test image pixels and is defined by

$$MSE = 1/mn \sum_{1}^{m}\sum_{1}^{n}[I_{ij} - I'_{ij}]^2 \quad (1)$$

$$PSNR = 20*log_{10}(\, max_f \,/\, sqrt(MSE)) \quad (2)$$

Legend: I-original image of size m*n. I'-recovered image of size m*n. max_f-maximum intensity value that exists in the original image (255).The higher the PSNR value, better the quality of the reconstructed image [3, 8].

5.2. Universal Image Quality Index (UQI)

It is defined by modeling the image distortion relative to the reference image as a combination of three factors: loss of correlation, luminance distortion, and contrast distortion.

$$UQI = 4\sigma_{xy}\,(xy)' \,/\, (\sigma_x^2 + \sigma_y^2)*(x'^2 + y'^2) \quad (3)$$

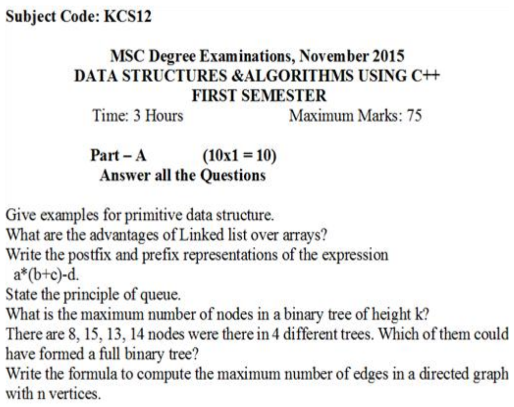
The range of values for the index UQI is [-1, 1]. The UQI value is if and only if the images are identical.

6. Experiments and Discussions

The proposed scheme is implemented on i5 Processor with 4 GB of memory using Matlab 10.0. The Question Paper is encrypted into two shares so that the original image is visible only when the two shares are overlaid using Exclusive-OR (XOR) operation. Figure 1 shows the input question paper, generated shares, signatures of the examiner and the recovered question paper is shown in Figure 1. The shares have the institution logo as an embedded watermark. As these shares contain the seal or logo of the institution or examination center, it is easy to identify the culprits leaking the question paper.

The proposed block based secret image sharing algorithm recovers the secret image with infinite PSNR value. The Visual cryptography (VC) schemes of Naor‘s [12] and Monoth [11] reconstructs only the half toned image with relative difference of black and white pixels as 1/2 and 5/8 respectively. However, the proposed scheme reconstructs the original image without any loss. Embedding the signature inside the shares for authentication degrades the quality of the recovered image with PSNR of 64.5dB. Table 1 shows the comparative analysis of the PSNR and Universal

Image Quality Index (UQI) for different file formats. The table shows that the PSNR and UQI of the images recovered using the proposed method for file formats other than .jpg is high when compared to the images in .jpg format. Table 2 shows the comparison PSNR and UQI of the recovered image in .jpg format for VC with half-toning method and the proposed method.

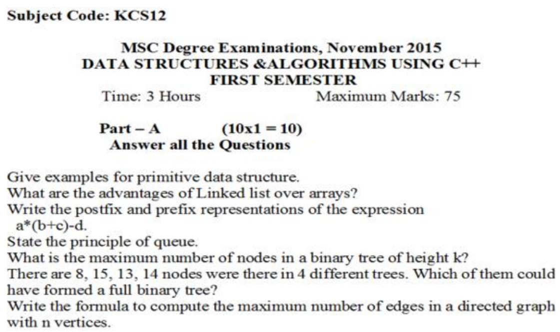

Subject Code: KCS12

MSC Degree Examinations, November 2015
DATA STRUCTURES &ALGORITHMS USING C++
FIRST SEMESTER
Time: 3 Hours Maximum Marks: 75

Part – A (10x1 = 10)
Answer all the Questions

Give examples for primitive data structure.
What are the advantages of Linked list over arrays?
Write the postfix and prefix representations of the expression
a*(b+c)-d.
State the principle of queue.
What is the maximum number of nodes in a binary tree of height k?
There are 8, 15, 13, 14 nodes were there in 4 different trees. Which of them could have formed a full binary tree?
Write the formula to compute the maximum number of edges in a directed graph with n vertices.

a) Input question paper image.

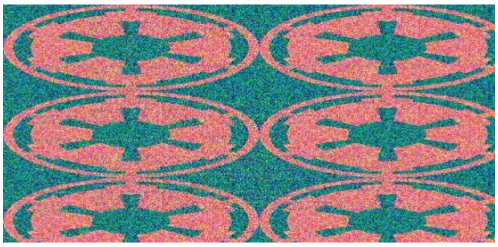

Subject Code: KCS12

MSC Degree Examinations, November 2015
DATA STRUCTURES &ALGORITHMS USING C++
FIRST SEMESTER
Time: 3 Hours Maximum Marks: 75

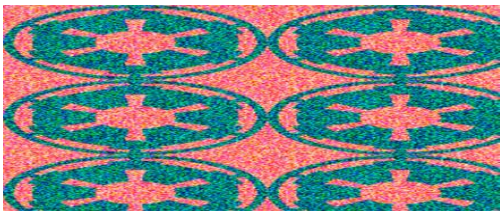
Part – A (10x1 = 10)
Answer all the Questions

Give examples for primitive data structure.
What are the advantages of Linked list over arrays?
Write the postfix and prefix representations of the expression
a*(b+c)-d.
State the principle of queue.
What is the maximum number of nodes in a binary tree of height k?
There are 8, 15, 13, 14 nodes were there in 4 different trees. Which of them could have formed a full binary tree?
Write the formula to compute the maximum number of edges in a directed graph with n vertices.

b) Recovered question paper image.



c) Share1.



d) Share 2.

e) Signature 1. f) Signature 2.

Figure 1. Experimental results for block based secret sharing scheme.

Symmetric key ciphers like Advanced Encryption Standard (AES) has gained acceptance as suitable for encrypting the data and is being implemented in secure file transfer protocols like File Transfer Protocol with SSL Security (FTPS), Hypertect Transfer Protocol Secure (HTTPS) because they require less resources. However, AES takes more time for decryption whereas the proposed algorithm takes less time to decrypt files as it involves simple XOR operation. Table 3 shows the performance of AES and proposed algorithm in terms of decryption time over different file size [14].

Table 1. Comparative analysis of PSNR and UQI for different file formats.

Image	Metrics	.png	.bmp	.tif	.jpg
Model1	PSNR	64.737	64.763	64.756	27.698
	UQI	0.985	0.985	0.985	0.120
Model2	PSNR	64.377	64.420	64.420	27.859
	UQI	0.969	0.969	0.969	0.126
Model3	PSNR	65.380	65.402	65.366	27.379
	UQI	0.965	0.965	0.964	0.106

Table 2. Comparative analysis of PSNR and UQI of proposed method and existing method.

	PSNR		UQI	
	Proposed Method	**Half toned VC**	**Proposed Method**	**Half toned VC**
Im1.png	64.737	24.268	0.985	0.003
Im2.tiff	64.763	24.207	0.985	0.003
Im3.bmp	64.756	24.186	0.985	0.003
Im4.jpg	27.69	24.343	0.120	0.003

Table 3. Decryption time of AES and proposed VC algorithm.

File Size	AES(ms)	Proposed Algorithm(ms)
100KB	31	3
500KB	101.7	6
1MB	186.7	7

7. Conclusions

This paper suggests the automation of examination system by securing question paper using secret sharing scheme. The main advantage of this proposed scheme with authentication is high visual quality of the color image with PSNR of 64.6dB, reduced computational complexity and no pixel expansion. The proposed method without authentication recovers the original image without any loss (PSNR value infinity) which is not possible with the existing visual cryptographic schemes. The alternative methods for authentication will further enhance visual quality of images. To the best of our knowledge, for the first time, color secret sharing scheme without half toning is applied for secure transmission of Examination question papers.

References

[1] Chen G., Liu J., and Wang L., "Color Image Sharing Method Based on Lagrange's Interpolating Polynomial," *in Proceedings of International Conference on Health Information Science*, Beijing, pp. 63-75, 2012.

[2] Cimato S., Prisco R., and Santis A., "Colored Visual Cryptography without Color Darkening,"

Theoretical Computer Science, vol. 374, no. 1-2, pp. 261-276, 2007.

[3] Fathimal M. and Jansirani A., "(N, N) Secret Color Image Sharing Scheme with Dynamic Group," *International Journal of Computer Network and Information Security*, vol. 7, no. 7, pp. 46-52, 2015.

[4] Fathimal M. and Jansirani A., "Bidirectional Serpentine Scan Based Error Diffusion Technique for Color Image Visual Cryptography," *International Journal of Science, Engineering and Technology Research*, vol. 3, no. 9, pp. 2255-2260, 2014.

[5] Fathimal M. and Jansirani A., "Design of Block based Visual Secret sharing Scheme for Color Images," *International Journal of Applied Engineering Research*, vol. 10, no. 33, pp. 26087-26091, 2015.

[6] Fathimal M. and Jansirani A., "K out of N Secret Sharing Scheme with Steganography and Authentication," *in Proceedings of Computational Intelligence, Cyber Security and Computational Models*, Singapore, pp. 413-424, 2015.

[7] Fathimal M. and Jansirani A., "K out of Secret Sharing Scheme for Gray and Color Images," *in Proceedings of IEEE International Conference on Electrical, Computer and Communication Technologies, Coimbatore*, pp. 1-4, 2015.

[8] Fathimal M. and Jansirani A., "Threshold based Region Incrementing Scheme for Color Images," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 9, no. 8, pp. 2049-2054, 2015.

[9] Guo C., Chang C., and Qin C., "A hierarchical Threshold Secret Image Sharing," *Pattern Recognition Letters*, vol. 33, no. 3, pp. 83-91, 2012.

[10] Kang I., Arce G., and Lee H., "Color Extended Visual Cryptography using Error Diffusion," *IEEE Transactions on Image Processing*, vol. 20, no. 1, pp. 132-145, 2011.

[11] Monoth T., Analysis and Design of Tamperproof and Contrast-Enhanced Secret Sharing Based on Visual Cryptography Schemes, Thesis, Kannur University, 2011.

[12] Naor M. and Shamir A., "Visual Cryptography," *in Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Saint-Malo, pp. 1-12, 1995.

[13] Shyu S., "Efficient Visual Secret Sharing Scheme for Color Images," *Pattern Recognition*, vol. 39, no. 5, pp. 866-880, 2006.

[14] Singhal N. and Raina J., "Comparative Analysis of AES and RC4 Algorithms for Better Utilization," *International Journal of Computer Trends and Technology*, pp. 177-181, 2011.

[15] Thien C. and Lin J., "Secret Image Sharing," *Computers and Graphics*, vol. 26, no. 5, pp. 765-770, 2002.

[16] Tu S. and Hsu C., "A Joint Ownership Protection Scheme for Digital Images Based on Visual Cryptography," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 276-283, 2012.

[17] Ulutas M., Ulutas G., and Nabiyev V., "Invertible Secret Image Sharing for Grey Level and Dithered Cover Images," *Journal of Systems and Software*, vol. 86, no. 2, pp.485-500, 2013.

[18] Verheul E. and Tilborg H., "Constructions and Properties of K out of N Visual Secret Sharing Schemes," *Designs, Codes and Cryptography*, vol. 11, no. 2, pp. 179-196, 1997.

[19] Wu X., Ou D., Liang Q., and Sun W., "A User-Friendly Secret Image-Sharing Scheme with Reversible Steganography Based on Cellular Automata," *Journal of Systems and Software*, vol. 85, no. 8, pp. 1852-1863, 2012.

[20] Yang C. and Laih C., "New Colored Visual Secret Sharing Schemes," *Designs, Codes and Cryptography*, vol. 20, no. 3, pp. 325-336, 2000.

[21] Yang C., Ouyang J., and Harn L., "Steganography and Authentication in Image Sharing without Parity Bits," *Optics Communications*, vol. 285, no. 7, pp. 1725-1735, 2012.

Mohamed Fathimal received her BE and ME in Computer Science and Engineering from Manonmanium Sundaranar University, Tirunelveli, Tamilnadu. She has 10 years of teaching Experience. Currently she is pursuing Phd in Manonmanium Sundaranar University. Her research interests include Digital Image Processing and Information Security.

Arockia Jansirani graduated B.E in Electronics and Communication Engineering from Government College of Engineering, Tirunelveli, Tamil Nadu, India in 1996 and M.E in Computer Science and Engineering from National Engineering College, Kovilpatti, Tamil Nadu, India in 2002. She has been with the Department of Computer Science and Engineering, Manonmaniam Sundaranar University as Assistant Professor since 2003. She has more than ten years of teaching and research experience. She completed her Ph. D in Computer Science and Engineering from Manonmaniam Sundaranar University, Tamil Nadu, India in 2012. Her research interests include Digital Image Processing, Neural Networks and Data Mining.