International Journal of Recent Advances in Multidisciplinary Topics
Volume 2, Issue 6, June 2021
https://www.ijramt.com | ISSN (Online): 2582-7839

Fool Proof Examination System through Color Visual Cryptography

Sayali Wani[1*], Pranjal Sansare[2], Mansi Singh[3], Gayatri Waghchaure[4], Abhay Gaidhani[5]
[1,2,3,4]*Student, Department of Computer Engineering, Sandip Institute of Technology and Research Center, Nashik, India*
[5]*Professor, Department of Computer Engineering, Sandip Institute of Technology and Research Center, Nashik, India*

***Abstract*: This paper proposes a replacement system of foolproof examination by tamperproof e-question paper preparation and secure transmission using secret sharing scheme. The appliance is perfectly secure because the proposed method automatically embeds the corresponding institute lock in the shape of the key. As a result, it's 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 aside from authentication. The proposed method recovers the first secret image with none loss. The prevailing visual cryptographic scheme recovers half-toned secret image with average Peak signal-to-noise (PSNR) value 24dB. Further, it shall be stated that the proposed method with authentication recovers the image with 64.7dB PSNR value, which is bigger than that of the prevailing method. Additionally, this method doesn't suffer from pixel Expansion.**

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

1. Introduction

To achieve secure transmission of knowledge, usually the info is concealed using symmetric or asymmetric key cryptography, which involves high computation and price effective in encryption and decryption process. Our system proposes a security system for tamperproof e-question paper sharing scheme using simple arithmetic operations. The key sharing scheme has two categories–visual cryptography scheme and polynomial based secret sharing scheme. The most aim of our system is to beat this drawback by employing secret sharing scheme for this application. The most concept of the first 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 secret by combination of the share images apart from all of the shares.

2. Project Scope

The main aim of our system is to beat this drawback by employing secret sharing scheme for this application. The most concept of the first 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 secret by combination of the share images apart from all of the shares. The accuracy of the K-N share algorithm should be high and classification should be unambiguous.

3. Methodology

In k out of n visual cryptography scheme may be a sort of cryptographic technique where a digital image is split into n number of shares by cryptographic computation. Within the decryption process only k or quite k number of shares can reveal the first information [Here can form the first image]. But k number of shares can't reveal the first information. During this paper we've proposed an algorithm to divide a digital color image into n number of shares where minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining shares are (n−k). In a picture if certain position of a pixel is 1, then in (n−k) +1 number of shares therein position of that pixel there'll be 1. Within the remaining shares therein position of the pixel there'll be 0. A random number generator is employed to spot those number of shares. The Question Paper is encrypted into two shares in order that the first image is visible only the 2 shares are overlaid using Exclusive-OR (XOR) operation. The input question paper, generated shares, signatures of the examiner and therefore the recovered question paper. 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's easy to spot the culprits leaking the question paper.

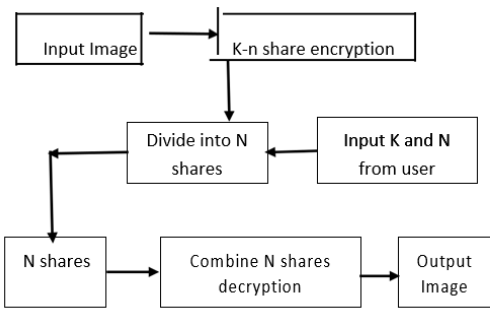

Fig. 1. System model

*Corresponding author: sayali.wani49@gmail.com

1) K-n Secret Sharing Visual Cryptography Scheme:

An image is taken as input. The amount of shares the image would be divided (n) and number of shares to reconstruct the image (k) is additionally taken as input from user. The division is completed by the subsequent algorithm. Step I: Take a picture IMG as input and calculate its width (w) and height (h).

- Step I: Take a picture IMG as input and calculate its width (w) and height (h).
- Step II: Take the amount of shares (n) and minimum number of shares (k) to be taken to reconstruct the image where k must be but or adequate to n. Calculate RECONS = (n-k) +1.
- Step III: Create a 3 dimensional array IMG_SHARE[n] [w*h] [32] to store the pixels of n number of shares. K-n secret sharing visual cryptographic division is completed by the subsequent process.

```
for i = 0 to (w*h-1)
{
Scan each pixel value of img and convert it into 32 bit binary string let pix_st. for j = 0 to 31
{
If (pix_st.charat(i) =1)
{
Call random place (n, recons)
}
for k = 0 to (recons−1)
{
set img_share [rand[k]][i][j] = 1
}
}
}
```

2) Enveloping Using Watermarking

Using this step the divided shares of the first image are enveloped within other image. Least Significant Bit (LSB) replacement digital watermarking is employed for this enveloping process. it's already discussed that a 32 bit digital image pixel is split into four parts namely alpha, red, green and blue; each with 8 bits. Experiment shows that if the last two bits of every of those parts are changed; the changed color effect isn't sensed by human eye [6]. This process is understood as invisible digital watermarking [7]. For embedding 32 bits of a pixel of a divided share, 4 pixels of the envelope image is important. It means to envelope a share with resolution w X h; we'd like an envelope image with w X h X 4 pixels. Here we've taken each envelope of size 4w X h.

3) Decryption Process

In this step a minimum of k numbers of enveloped images are taken as input. From each of those images for every pixel, the last two bits of alpha, red, green and blue are retrieved and OR operation is performed to get the first image. It's already discussed that human sensory system acts as an OR function. For computer generated process; OR function are often used for the case of stacking k number of enveloped images out of n.

4. Results

1) Login page

When we open the system application user need to login. The subsequent image contains the results of login into the appliance.

Fig. 2. Login page

2) Division using Visual Cryptography

An image is taken as input. The amount of shares the image would be divided (n) and number of shares to reconstruct the image (k) is additionally taken as input from user.

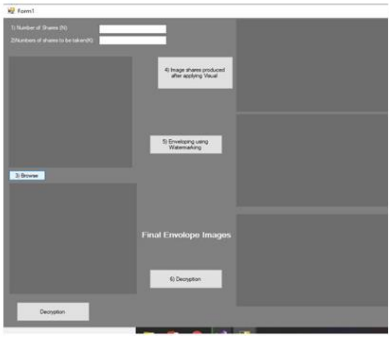

Fig. 3. User input

3) Enveloping image

Using this step the divided shares of the first image are enveloped within other image.

Fig. 4. Enveloping image

Fig. 5. Decryption

4) Decryption Process

In this step a minimum of k numbers of enveloped images are taken as input. Construct pixel from these part and store it into final image.

5. Conclusion

Our system suggests the automation of examination system by securing question paper using secret sharing scheme. The choice methods for authentication will further enhance visual quality of images. To the simplest of our knowledge, color secret sharing scheme without half toning is applied for secure transmission of Examination question papers. The division of an image into n number of shares is done by using random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography.

References

[1] Singh, Vineet Kumar, Piyush Kumar Singh, and K. N. Rai. "Image Encryption Algorithm supported Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.

[2] Maurya, R., Kannojiya, A. K., & Rajitha, B. (2020). An Extended Visual Cryptography Technique for Medical Image Security. 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020.

[3] Munir, R., & Harlili.. Encryption by Using Visual Cryptography supported Wang's Scheme. 2018 4th International Conference on Electrical, Electronics and System Engineering (ICEESE), 2018.

[4] Li, P., Ma, J., Yin, L., & Ma, Q. A Construction Method of (2, 3) Visual Cryptography Scheme, 2020.

[5] B. Shrivas and S. Yadav "Visual Cryptography within the Video using Halftone Technique" International Journal of Computer Applications (0975 – 8887) vol. 117 no. 14 May 2015.

[6] Zhou, Z., Yang, C.-N., Cao, Y., & Sun, X. (2018). Secret Image Sharing supported Encrypted Pixels. IEEE Access, 6, 15021– 15025, 2018.

[7] K.Shankar, P. Eswaran, Sharing a Secret Image with Encapsulated Shares in Visual Cryptography, Procedia computing, vol. 70, 2015.

[8] Singh, V. K., Singh, P. K., & Rai, K. N. (2018). Image Encryption Algorithm supported Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images. 2018 4th International Conference on Computing Communication and Automation (ICCCA).

[9] K. Shankar and P. Eswaran, RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique, J circuit syst comp 25, 1650138, 2016.