VARIABLE LENGTH KEY BASED VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE

Akhil Anjikar [1], Prashant Dahiwale[2], Suchita Tarare [3]

[1]Deparment of Information technology,
Rajiv Gandhi college of Engineering & Research, Nagpur, India.
akhil.anjikar09@gmail.com
[2]Department of Computer Sci. & Engg.,
Rajiv Gandhi college of Engineering & Research, Nagpur, India.
prashant.dahiwale@gmail.com
[3]Department of Computer Sci. & Engg.,
Rajiv Gandhi college of Engineering & Research, Nagpur, India.
suchitatarare@gmail.com

ABSTRACT

Visual Cryptography is a special encryption technique that encrypts the secret image into n number of shares to hide information in images in such a way that it can be decrypted by the human visual system. It is imperceptible to reveal the secret information unless a certain number of shares (k) or more are superimposed. Simple visual cryptography is very insecure.

Variable length key based visual cryptography for color image uses a variable length Symmetric Key based Visual Cryptographic Scheme for color images where a secret key is used to encrypt the image and division of the encrypted image is done using Random Number. Unless the secret key, the original image will not be decrypted. Here secret key ensures the security of image.

This paper describes the overall process of above scheme. Encryption process encrypts the Original Image using variable length Symmetric Key, gives encrypted image. Share generation process divides the encrypted image into n number of shares using random number. Decryption process stacks k number of shares out of n to reconstruct encrypted image and uses the same key for decryption.

KEYWORDS

Visual Cryptography, Secret Sharing, Random Number, Symmetric Key.

1. INTRODUCTION

Cryptography is study of mathematical technique to provide the methods for information security. It provides such services like authentication, data security, and confidentiality. Visual cryptography is one of the techniques used in modern world to maintain the secret massage transmission. In this technique no need of any cryptographic algorithms likes symmetric (DES, AES, TRIPLE DES etc) and asymmetric (RSA, Diffie- Hellman, Elliptic Curve Cryptographic) algorithms. Noar and Shamir introduce visual cryptography in 1994 [2]. This technique is used to

David C. Wyld et al. (Eds) : SAI, CDKP, ICAITA, NeCoM, SEAS, CMCA, ASUC, Signal - 2014
pp. 97–104, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.41110

reduce complexity of encrypted and decrypted method and also two way communication can be achieved very securely. Traditional techniques use private and public key concepts. But it could be achieved only by the distribution of keys [7].

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg. Image is a multimedia component sensed by human perception. A color digital image is composed of a finite number of elements called pixels. In a 24 bit digital image each pixel consists of 24 bits, which includes three parts, namely Red, Green and Blue, each with 8 bits [1][2].

Human visual system acts as an OR function. If shares are printed on transparencies and stack together then anyone can visualize the image. To make it more secure we are using variable length symmetric key. Fixed length key can be easily computed by combination of characters by the attacker. For variable length key, it is difficult to find the key as the length can be 0 to any number.

A Key is used to provide more security so that attacker cannot retrieve the secret information without the key. Original image is encrypted using key and produces cipher. Cipher is decrypted using key and the original image is retrieved. Same key is used for encryption and decryption called symmetric encryption.

2. LITERATURE REVIEW

Visual cryptography proposed by Naor and Shamir where encryption of image means the generation of shares without any cryptographic computation. Original image is divided into n number by shares by applying any k-n secret sharing visual cryptographic scheme. Decryption is done by human visual system means if shares are printed on transparencies and stack together then anyone can visualize the image. So, if anyone get some number of shares can easily decrypt the image. Simple visual cryptography is not very secure technique [1].

Watermarking using visual cryptography where original image is divided into shares, with k-n secret sharing visual cryptography scheme. An enveloping technique is proposed where the secret shares are enveloped within apparently innocent covers of digital pictures using LSB replacement digital watermarking. This adds security to visual cryptography technique from illicit attack as it befools the hacker’s eye. K-n secret sharing process is simple as random number is used. Shares contain the original image contents, if anyone get shares then original image can be obtained [10].

The shares are enveloped into apparently innocent cover of digital pictures and can be sent through same or different communication channels. Invisible digital watermarking befools the hacker. Watermarking is a technique to put a signature of the owner within the creation. As shares are generated from the original image this scheme does not provide more security [2].

3. PROPOSED WORK

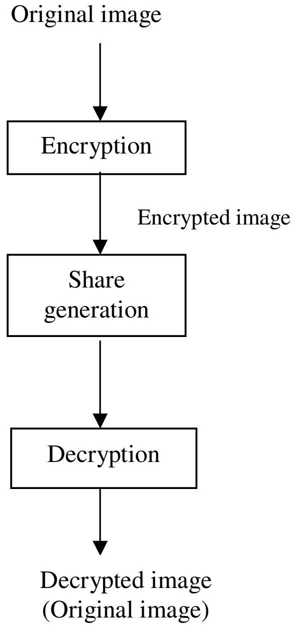


Figure 1. Overall process

3.1. Module – 1

Image encryption using secret key

Original image is encrypted using key. A user generated any combination of characters of varying length gives a key. Generated key and original image are taken as input. Pixel array is computed from original image and key is XOR ed with pixel array to give encrypted image. The contents of original image and encrypted image are totally different, this process makes encrypted image blur to some extent and provide security.

- Take original image as a input; calculate width and height

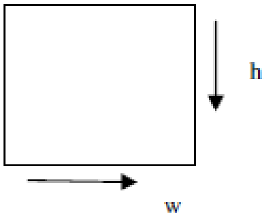


Figure 2. Original image

- Convert each pixel into 24-bit binary , so size of image is (w*h*24)

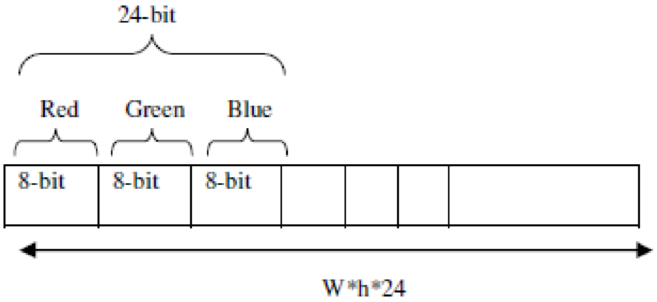


Figure 3. 24-bit converted image

- Enter key from user and calculate length also calculate 7 bit binary string
  Let key is: **abcdef** length of key is**:** 6

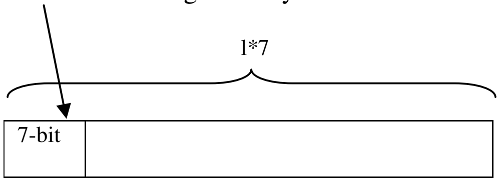


Figure 4. 7-bit binary String Key

- XOR 24-bit converted image and 7-bit binary string key

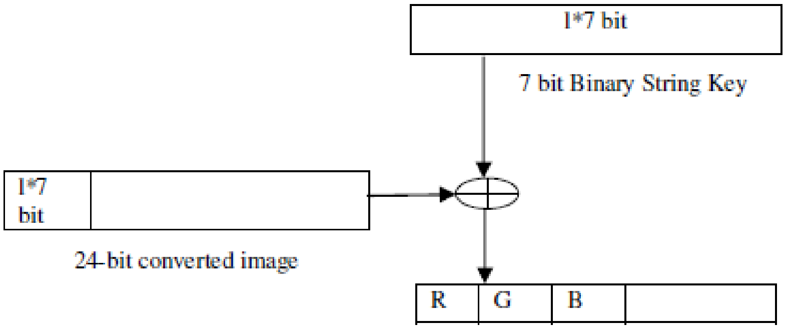


Figure 5. 24-bit encrypted image

- Now the 24-bit encrypted image is reconstructed to get Encrypted image of size equal to original image size

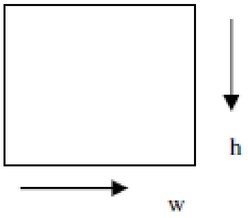


Figure 6. Encrypted image

3.2. Module - 2

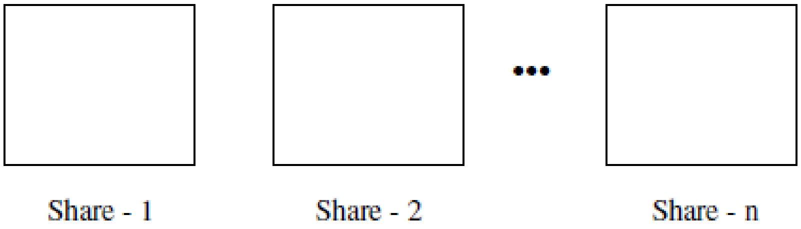
Division of encrypted image

The encrypted image is then divided into n number of shares using k-n secret sharing visual cryptography scheme i.e. using Random Number such that the size of shares equals original image size. K number of shares is sufficient to reconstruct the encrypted image. k number of shares produced is stacked together to reconstruct the encrypted image. Decryption is impossible until the k number of shares are available.

- Enter the number of shares you want to create, suppose n
  and shares required for reconstruction are k

  Calculate recons = (n-k)+1

- N number of shares equal to 24-bit converted image size will be created.
- Take the encrypted image as input and convert it into 24-bit encrypted image.
- Scan each bit of 24-bit encrypted image and check for bit 1, if bit is 1 then Random number generator will generate different numbers in the range 1 to n, (numbers generated will be equal to recons).
- 1 is put in generated shares at the same position as in 24-bit encrypted image.
- The same procedure is followed until total bits are scanned.
- Then all the shares are reconstructed to make it equal to original image size.



3.3. Module – 3

Image decryption using secret key

The decryption process consists of two steps. First step is done by human visual system where at least k number of shares out of n number of shares is superimposed to give reconstructed image. Human visual system acts as an OR function. For computer generated process,OR function can be used for the case of stacking k number of shares out of n. Second step is decryption of reconstructed image, where pixel array is computed from reconstructed image and XOR ed with same key used for encryption. Decrypted image is exactly equal to original image.

- Input the number shares you have and the same key used for encryption.
  Shares should be equal to k or greater than k
- Perform the bitor operation on converted shares to ger reconstructed encrypted image.
- Now XOR the reconstructed encrypted image and converted key to get 24-bit decrypted image, it then reconstructed to give decrypted image equal to original image.

3. RESULT

3.1. Encryption Process:

Original Image: onion.png
Source image is

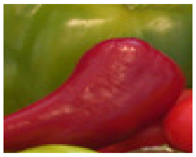


Figure 7. Original Image

Secret Key is : **testing**

The Encrypted Image :

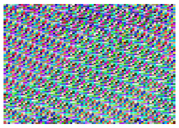
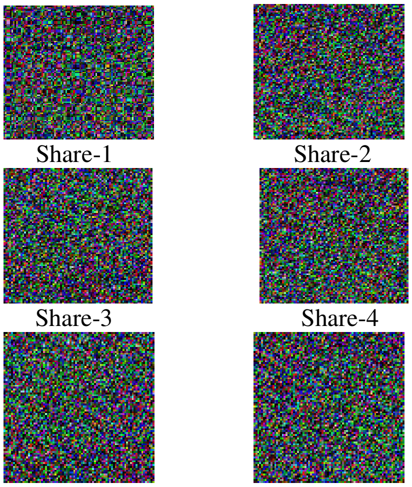


Figure 8. Encrypted Image

3.2. Division of image into number of shares

Number of Shares (n): 6

Numbers of shares for reconstruction (k): 4



Share-1 Share-2
Share-3 Share-4
Share-5 Share-6

Figure 9. Image shares produced after applying k-n Visual Cryptography

3.3. Decryption Process

Number of shares taken for reconstruction: 4

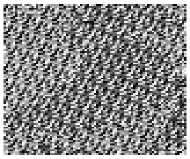


Figure 10. Reconstructed Image

Secret Key is: **testing**
Key is applied on reconstructed image. The Final image is:

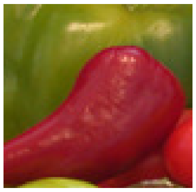


Figure 11. Decrypted Image

4. CONCLUSION

In visual cryptography encryption means the generation of shares and decryption in is based on OR operation, so if a person gets sufficient k number of shares the image can be easily decrypted. So simple visual cryptography is not more secure.

In this paper we have proposed a variable length key based visual cryptography for color image with random number for share generation. In this scheme key adds robustness to the visual cryptography techniques and variable length of the key makes it more secure. Generated shares have totally different information regards to original image. For share generation we are using random number which needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images [3][4][5]. As we are using variable length key for encryption and random number generator for share generation this process is more secure than other visual cryptography schemes [8].

Table 1. Comparison of other processes with Proposed Scheme

Other processes	**Proposed scheme**
Share generation process is applied directly on original image.	Share generation process is applied on encrypted image.
Generated shares contain the original image contents.	Generated shares have totally different contents.
Do not provide more security.	Use of key makes it more secure.
Share generation process is complex.	Share generation process is simple as random number is used.
Decryption is done by OR operation.	Decryption is done by OR as well as XOR operation.

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography,”Advances in Cryptology-Eurocrypt‟94, pp.1–12, 1995.

[2] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, Vol16, No.4 May 1998, pp.573–586.

[3] F. Liu1, C.K. Wu1, X.J. Lin, Colour visual cryptography schemes, IET Information Security, July 2008.

[4] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diffusion, IEEE 2010.

[5] SaiChandana B., Anuradha S., A New Visual Cryptography Scheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.

[6] Li Bai , A Reliable (k,n) Image Secret Sharing Scheme by, IEEE,2006.

[7] M.Amarnath Reddy, P.Shanthi Bala, G.Aghila “visual cryptography schemes comparision”, Vol. 3 No. 5 May 2011.

[8] SaiChandana B., Anuradha S., A New Visual Cryptography Scheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.

[9] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diffusion, IEEE 2010.

[10] JIM CAI, “ A SHORT SURVEY ON VISUAL CRYPTOGRAPHY SCHEMES”.