*International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622*
*International Conference on Industrial Automation And Computing (ICIAC-12th &13th April 2014)*

RESEARCH ARTICLE OPEN ACCESS

# Comparative study of Variable length key based visual cryptography and Visual Cryptography with Enveloping by Digital Watermarking.

Suchita Tarare[1], Akhil Anjikar[2], Hemant Turkar[3]

[1](Department of Computer Sci. & Engg., Rajiv Gandhi college of Engineering & Research, RTMNU Nagpur University, India. Email: suchitatarare@gmail.com)

[3](Department of Information Technology, Rajiv Gandhi college of Engineering & Research, RTMNU Nagpur University, India. Email: akhilanjikar09@gmail.com)

[3](Department of Computer Sci. & Engg., Rajiv Gandhi college of Engineering & Research, RTMNU Nagpur University, India. Email: hemantturkar@rediffmail.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. To reveal the secret information at least a certain number of shares (k) or more are superimposed.

In Visual Cryptography with Enveloping by Digital watermarking Scheme for color images, where the divided shares are enveloped in other images using invisible digital watermarking and the shares are generated using Random Number. Variable Length Key based Visual Cryptography Scheme for color images, where a secret key is used to encrypt the image and division is done using Random Number. Unless the secret key, the original image will not be decrypted. This paper compares these two visual cryptography schemes in terms of security, quality of images.

***Keywords –*** Visual Cryptography, Symmetric Key, Digital Watermarking, Random Number.

## I. INTRODUCTION

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. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. Visual cryptography is one of the solution for Encryption. Visual cryptography is proposed in 1994 by Naor and Shamir who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS) [1].

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 technique 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 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.

### 1.1. Variable length key based visual cryptography

In variable length Symmetric Key based Visual Cryptographic Scheme for color images where a secret key is used to encrypt the image. Division of the encrypted image is done using k-n secret sharing visual cryptographic scheme i.e. using Random Number. It is imperceptible to reveal the secret information unless a certain number of shares (k) or more are superimposed. Unless the secret key, the original image will not be decrypted. Here secret key ensures the security of the scheme and visual cryptography is used to break the image into number of shares [8] [9].

### 1.2. Visual Cryptography with Enveloping by Digital Watermarking

Original image is divided into number of shares, produced by k-n secret sharing visual cryptography are embedded into the envelope images by LSB replacement [3]. The color change of the envelope images are not sensed by human eye [4]. (More than 16.7 million i.e.224 different colors are produced by RGB color model. But human eye can discriminate only a few of them.). This technique is known as invisible digital watermarking as human eye cannot identify the change in the envelope image and the enveloped (Produced after LSB replacement) image [5]. In the decryption process k number of embedded envelope images are taken and LSB are retrieved from each of them followed by OR operation to generated the original image.

## II. ANALYSIS OF THESE METHODS

### 2.1. Variable length key based visual cryptography

Key is used to encrypt the original image, key makes the image blur. K-n secret sharing scheme is applied on encrypted image, that is shares are generated from the encrypted image. Secret key which makes the technique more robust. Visual Cryptography technique makes an illusion to the hacker's mind to protect secret information encoded in an image. Here the shares and the key are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes. Here the main part is using a key. Key in the text format may arise suspicion to the hacker's mind that some secret information is passed. Shares do not contain original image's contents, so if anyone get shares then also the decryption is impossible as it requires the same key used for encryption.

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 on color images [9][10] [11]. This technique only checks '1' at the bit position and divide that '1' into (n-k+1) shares using random numbers.

Decryption is done by OR as well as XOR with the key, which make it more secure.

### 2.2. Watermarking using visual cryptography

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.

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.

## III. CONCLUSION

This paper compares the Variable length key based visual cryptography and Watermarking using visual cryptography with the advantages and disadvantages of both schemes.

Variable length key based visual cryptography provide more security by changing the actual contents of original image but give meaningless shares where as Watermarking using visual cryptography do not provide more security but give meaningful shares and put a signature of the owner within the creation.

**TABLE-I**
**Comparison of two processes**

| Sr. No. | Variable length key based visual cryptography | Variable length key based visual cryptography |
|---|---|---|
| 1. | Secret key is used to encrypt the image, key makes the image blur. | Image is not Encrypted. |
| 2. | K-n secret sharing process is applied on encrypted image. | K-n secret sharing process is applied on original image. |
| 3. | Meaningless shares are generated. | Shares generated are meaningful |
| 4. | Decryption is done by OR as well as XOR | Decryption is done by OR. |

| | | |
|---|---|---|
| | with the key. | |
| 5. | Key in the text format may arise suspicion to the hacker's mind that some secret information is passed, the shares and the key are sent through different communication channels from sender to receiver. | 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. |

## IV. FUTURE WORK

Variable length key based visual cryptography provide more security by changing the actual contents of original image but give meaningless shares where as Watermarking using visual cryptography do not provide more security but give meaningful shares and put a signature of the owner within the creation.

Combining advantages of both the schemes we can develop new technique which can adds security to visual cryptography technique from illicit attack and also give meaningful shares which can befools the hacker.

## REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography,"Advances in Cryptology-Eurocrypt 94, pp. 1–12, 1995.
[2] M.Amarnath Reddy, P.Shanthi Bala, G.Aghila "visual cryptography schemes comparision", Vol. 3 No. 5 May 2011
[3] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010, pp 62-65.
[4] Hartung F., Kuttter M., "Multimedia Watermarking Techniques", IEEE, 1999.
[5] 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,.
[6] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, 1995, pp. 1–12.
[7] Krishmoorthy R, Prabhu S, Internet & Java Programming, New Age International, pp 234.
[8] F. Liu1, C.K. Wu1, X.J. Lin, Colour visual cryptography schemes, IET Information Security, July 2008.
[9] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diffusion, IEEE 2010
[10] SaiChandana B., Anuradha S., A New Visual Cryptography Scheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.