Encryption of Images by Random Grids: An Overview

1Prof. Kapil Tajane, 2Prof. Rahul Pitale, 3Mr. Mayur Tajane
1Department of Information Technology, D. Y. Patil College of Engineering, Akurdi, Pune.
2Department of Computer Engg, Nutan Maharashtra Institute of Technology, Talegaon Dabhade, Pune.
3Senior Project Associate Cognizant Technology Solutions, Pune.
kapiltajane@gmail.com, rahulpitale3@gmail.com, mayur.tajane@gmail.com

ABSTRACT

Visual cryptography (VC) is a cryptographic technique which allows visual information such as images to be encrypted in such a way that the decryption can be performed by the human visual system, without the use of computers. The well-known technology that encrypts a secret image into multiple share images is Visual Secret Sharing (VSS). When we superimpose these shares, it can restore the secret image by human vision only. It’s well-known that visual secret sharing aims at encrypting a secret image into number of meaningless sharing images by either designing a well-designed codebook or generating random bit sequence and then reconstructing the secret by superimposing them without any computation. But, the traditional visual secret sharing schemes encrypts only one secret at a time. But later on different authors or researchers has proposed different algorithm to encrypt two or more images at a time using random grid. The intent of this paper is to provide an analysis of some existing image encryption methods using random grids. We have compared all these schemes based on some parameters.

Index Terms: Decryption, Encryption, Random Grids, Secret Sharing, Visual Cryptography

I. INTRODUCTION

With the fast growth and advancement of network technology, multimedia information is transmitted over the internet conveniently. Various important and confidential data such as military maps and commercial or stock market related data are transmitted over the internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To recover the security problems of secret images, various image secret sharing schemes have been developed. In 1994, Naor and Shamir has firstly introduced visual cryptography (VC) [1]. Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system, without the use of computers. Visual cryptography scheme reduces complex computation problem in decryption process, and the secret images can be restored by superimposing shares. This property makes visual cryptography especially useful for the low computation load requirement. Blakley and Shamir were first who introduced the concept of Secret Sharing Scheme (SSS) to solve the master key sharing problem [2]. Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n participants. The most important property of visual cryptography is that, the decryption of the secret images does not require the knowledge of cryptography and complex computation, because a human visual system is used to decode the secret. Hence we can easily recover the secret by using human eye only without the help of any computing devices. The following Fig. 1 shows (2,2) visual cryptography scheme. In this paper, in section II literature survey of various image encryption methods is carried out. In section III comparative analysis of all methods based on some parameters is given. And at last in section IV conclusion of study is given.
II. LITERATURE SURVEY CRUX

Naor and Shamir[3]

Naor and Shamir’s are 1st who proposed method for binary image encryption into two shares that is Share1 and Share2. If pixel is white one of the above two rows are chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows are chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each of share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both of the images became shares are superimposed. This scheme is shown in Fig. 1. But this method has pixel expansion in shares and reconstructed image. It requires computation steps for decoding secret.

Wu and Chang[4]

In this paper author has proposed a new scheme known as "sharing visual multi-secrets using circle shares" based on visual cryptography. In this scheme author has encrypted two images but generated shares are circular in shape. It reduces the limitation of angle of rotation for restoring the second secret image. As compared with traditional visual cryptography, this technique has more flexibility, extensibility and security. But this method has pixel expansion in shares and reconstructed image. It requires computation steps for decoding secret.

Shyu et al.[5]
In this paper author has proposed a new scheme which encrypts four images at a time in two shares based on visual cryptography. The generated shares are circular in shape. Here shares are having marking line to overlap the shares to restore images. Share1 has 3 lines at 0°, 120° and 240°. Share2 has marking line at 0° only. So depending upon the marking we have to overlap shares and we will be able to restore 4 secret images. But this method has pixel expansion in shares and reconstructed image. It requires computation steps for decoding secret.

Feng et al.[6]

In this paper author has proposed novel visual secret sharing scheme for multiple secret images. The number of secret images are not restricted and they are encrypted in two shares only. Depending upon the variation of angle the different secret image will get restored. The angle of variation is depend on the number of secret images encrypted. But this method has pixel expansion in shares and reconstructed image. It requires computation steps for decoding secret.

Kafri and Karen[7]

In this paper author has introduced image encryption by random grids firstly. Random grids are nothing but the transparency comprising a two dimensional array of pixels. The encoding method is same as that of visual cryptographic methods but decoding is done in single step that is by superimposing random grids we are able to restore secret image by our visual system. Advantage of this method over visual cryptographic methods is no pixel expansion and no code book requirement. In this scheme single secret image is encrypted into two shares.

Shyong Jian Shyu[8]

In this paper author has proposed image encryption method based on random grids for gray-level and color images. At a time one secret image is encrypted into two cipher grids. For restoring secret image we have to superimpose both cipher grids. The problem of pixel expansion and codebook design is removed as compare to visual cryptography.

Chen et al.[9]

In this paper author has proposed image encryption method based on random grids. At a time two secret images are encrypted into two cipher grids. For restoring first secret images we have to superimpose both cipher grids then for restoring second secret image keep cipher grid1 as it is and rotate cipher grid 2 by 90°. By human visual we are able to get both secret images. In this scheme, size of cipher grid and reconstructed secret image is same as that of original secret image. The problem of pixel expansion and codebook design is removed as compare to visual cryptography.

Joy Jo-Yi Chang et al.[10]

In this paper author has proposed image encryption method based on random grids. At a time two secret images are encrypted into two cipher grids. For restoring first secret images we have to superimpose both cipher grids then for restoring second secret image keep cipher grid1 as it is and move cipher grid2 horizontally. By human visual we are able to get both secret images. These scheme is used for any rectangular secret images. The distortion of second restored image is less as compare to [9]. In this
scheme, size of cipher grid and reconstructed secret image is same as that of original secret image. The problem of pixel expansion and codebook design is removed as compare to visual cryptography.

Chen et al.[11]
In this paper author has proposed image encryption method based on random grids. At a time multiple secret images are encrypted into two cipher grids. For restoring first secret images we have to superimpose both cipher grids then for restoring second secret image keep cipher grid1 as it is and rotate cipher grid2 by \((360^\circ/m)\)*(k -1) , (k=1,2,...,m) degrees. By human visual we are able to get all secret images. In this scheme, size of cipher grids and reconstructed secret images is same as that of original secret image. The problem of pixel expansion and codebook design is removed as compare to visual cryptography.

III. COMPARATIVE STUDY

Few image encryption schemes are considered for comparative study based on some parameters. The following table summarizes that:

<table>
<thead>
<tr>
<th>Encryption Schemes</th>
<th>Year</th>
<th>Pixel Expansion</th>
<th>Codebook Design</th>
<th>Number of Secret Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naor and Shamir[3]</td>
<td>1995</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td>Wu and Chang[4]</td>
<td>2005</td>
<td>Yes</td>
<td>Yes</td>
<td>2</td>
</tr>
<tr>
<td>Shyu et al.[5]</td>
<td>2007</td>
<td>Yes</td>
<td>Yes</td>
<td>4</td>
</tr>
<tr>
<td>Feng et al.[6]</td>
<td>2008</td>
<td>Yes</td>
<td>Yes</td>
<td>m</td>
</tr>
<tr>
<td>Kafri and Karen[7]</td>
<td>1987</td>
<td>No</td>
<td>No</td>
<td>1</td>
</tr>
<tr>
<td>Shyong Jian Shyu[8]</td>
<td>2006</td>
<td>No</td>
<td>No</td>
<td>1</td>
</tr>
<tr>
<td>Chen et al.[9]</td>
<td>2008</td>
<td>No</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>Joy Jo-Yi Chang et al.[10]</td>
<td>2010</td>
<td>No</td>
<td>No</td>
<td>m</td>
</tr>
<tr>
<td>Chen et al.[11]</td>
<td>2010</td>
<td>No</td>
<td>No</td>
<td>m</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

The different image encryption techniques based on visual cryptography and random grids are studied. The comparative study of all methods is done with respect to specific parameters. This paper will give the brief idea about different image encryption methods.

V. REFERENCES


