RESEARCH ARTICLE OPEN ACCESS

# A New Approach to Encrypt Grayscale Images using Visual Cryptography

U. Udayakumar [1], G.S. Gayathri [2], K. Vijayarangan [3]
Department of Computer Science
SRM Institute of Science and Technology, Chennai
TamiNadu – India

**ABSTRACT**
In today's advanced technology, every sensitive data must be secured. Visual cryptography is a technique to hide image based secrets. This paper suggests a method by which the secret image and the key feature of visual cryptography are encrypted into two phases simultaneously at decryption side, the secret image is revealed. This process uses the Latin square basic structure to avoid duplications in visual cryptography. Further, it applies visual cryptography scheme on gray image instead of on binary image. Decrypted image has the same size as the original secret image.
*Keywords :—* Secret Image, Latin square, Visual Cryptography Scheme, Visual Cryptography.

## I. INTRODUCTION

Visual Cryptography is a special encryption technique to hide information in images such that it can be decrypted by human vision if the correct key image is used. The original information to be encrypted is referred to as secret. Once encryption is completed, ciphers are generated, which are referred to as shares. To split the secret among a group of 'n' participants is the fundamental idea behind visual cryptography. The secret is divided into 'n' number of earlier, it says ciphers are called shares in order to split he secret. These shares are distributed among 'n' participants. Each participant provides his/ her own share, and all the shares are combined to reveal the original secret. With the advance of computer science and technology, the circulations and exchanges of information have created challenges to data security and cryptography. Visual Cryptography (VC) is a branch of secret sharing. In the VC scheme, a secret image is encoded into 2 or more transparencies.

Fig. 1 Examples of visual cryptography (a) Original image, (b) and (c) over layered encrypted, (d) the superposed (b) and (c) giving the result.

Using any one transparency, the content cannot be deciphered to reveal/show the original image, while the two transparencies Fig.1 (b) and (c) create the original image when overlaid, as shown as in Fig.1 (d).

## II. LITERATURE SURVEY

Visual cryptography is an image encryption technique to hide the image-based secret. The main advantage of visual cryptography is that it does not require any complex computation for decryption of secret; the human visual system is adequate. Visual cryptography, introduced by MoniNaor and Adi Shamir in 1994. Visual cryptography is a special kind of cryptographic technique which can decode concealed images without using any cryptographic computation [1]. It involves breaking up the image into 'n' shares so that only 'authenticated user' with all 'n' shares can decrypt the image by overlaying all the shares over each other with proper orientation.

P. V. Chavan et al. [2] have introduced a new concept for secret image sharing. Hierarchical visual cryptography hides the secret information into multiple levels. The expansion ratio of this technique is 1:4. In [3], a new visual secret sharing scheme was introduced by researchers, by which secret image was encoded into multiple levels and Gray scale image was an input to the system. This Gray scale image was transformed into half-tone image using half toning process, after which kernel's algorithm was applied on half-tone image—which was based on histogram of secret image obtained by securing the frequency of each Gray value—by which two shares were generated.

In [4], a new scheme was proposed (2, 2) and (3, 3) visual cryptography for Gray scale image. These researchers used randomization and pixel reversal approach for all methods [4]. In [5], authors proposed the design of hierarchical visual cryptography, by which secret image was divided into two shares, which independently generated their own two shares. The same method can apply on binary image that will retrieve by using more iterations than Gray image. In [6], authors developed a new signature-based authentication system based on hierarchical visual cryptography algorithm mentioned in [5]. HVC encrypts the secret in 3 levels. Shares generated out

of HVC were used for authentication mechanism. All shares were high contrast in nature. Signature based authentication was found to be more reliable than biometric authentication as biometric patterns change over time. Shares generated with this scheme were random in nature, giving no information by visual inspection, and graying effect was reduced to zero due to high contrast nature of shares [6].

In [7], authors proposed Gray share generation of 'n' number of shares. In [8], authors proposed a text form visual sharing scheme. Differing from traditional visual sharing scheme which use images, this method shares text files. In [9], authors proposed a novel method which first makes use of Latin square to prevent cheating in VC.

## III. PROPOSED WORK

We have designed a new scheme for visual cryptography using VC scheme technique to generate a secret key for encryption and decryption of images using multiple shares. This proposed scheme with VC uses two transparent images. One image contains random pixels; the other contains the secret information. It is impossible to retrieve the secret information from any one image. The overlay animation shows the 2 layers sliding over each other until they are correctly aligned and the hidden information appears. Both layers exactly fit over each other as shown in Fig.2. In this algorithm, final key mask is generated using systematic randomization with key, then the original secret image is fed as an input to the system.

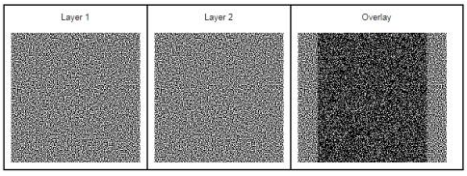


Fig. 2 Overlayered Image

***Encoding Algorithm***

```
Cipher text=bit of image XOR bit of key;
For(int i=0; i<strlen(Input Image); i++) // both encrypt and decrypt
{
Input[i] = key;
}
Encrypt(char key, char image, size)
{
For(int i=0; i< 1; i++)
Image[i]= key;
}
Decrypt(char key, char image, size)
{
Encrypt(key, image, 1)
}
```

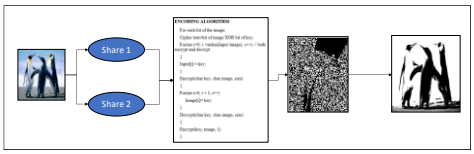


Fig. 3 Encoding Algorithm

## IV. EXPERIMENTAL RESULT

The experimental result of proposed scheme of gray visual cryptography is shown below. Fig.3 shows the original secret image. Fig.4 shows single phase of encryption share 1 and share2. Fig.5 shows decrypted image. Decrypted image has the same size as, and better visual quality than, the original secret image. This technique produces, two black and white transparencies images with each transparency having 50% result to decipher the image. A one transparency cannot show the original image, while the two transparencies—Fig.4 overlaid the original image—is shown in Fig.5.

Any secret image to be sent is divided into shares. When these two shares are stacked with perfect orientation and seen by a Human Visual System, the resultant image is revealed. In the visual secret sharing model, a secret picture must be distributed among 'n' participants. The picture is divided into 'n' shares so that if and only if all 'n' transparencies (shares) are placed together will the picture be visible. When there are fewer than 'n' transparencies, it is not revealed. This ensures that the secret picture is viewed as a set of black and white pixels, with each pixel being handled separately.

Each share is printed in a transparency. A share is a random noise. Encryption is performed for each pixel. Fig.2 shows the 2 unique shares for black and white pixels; Every pixel in the image is divided into two sub pixels, depending on whether the pixel is black or white. This is termed as Pixel Expansion.

Consider a QR code as a black and white picture to be sent in a secure manner for accessing a website or link. Unless the full picture is transferred, the link is not revealed. So, if it is split into 2 or more parts, these will have to be overlaid perfectly to form the original QR. Instead of cutting a QR code into bits, it is also possible to consider it as a set of pixels, which are then available on different transparencies such that when all the transparencies are put together with the right orientation but in any order, the original code is visible. Each transparency will have white pixels, black pixels and blank spaces (where the pixels of other transparencies will be revealed). Further refinements and splitting of color pictures can be considered as possible developments.

TABLE I
SINGLE PHASE ENCRYPTION

| Algorithm | Single Phase Encryption |
|---|---|
| AES | 0.15 |
| DES | 0.22 |
| RSA | 0.16 |
| Proposed | 0.10 |

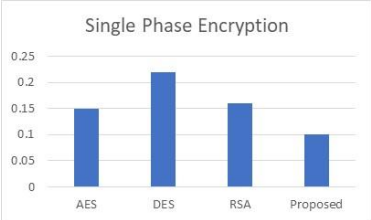


Fig. 4 Single Phase Encryption

TABLE III
DECRYPTED SECRET IMAGE

| Algorithm | Decrypted Secret Image |
|---|---|
| AES | 0.24 |
| DES | 0.38 |
| RSA | 0.27 |
| Proposed | 0.16 |


Fig. 5 Decrypted Secret Image

Fig. 6 Original Secret Image

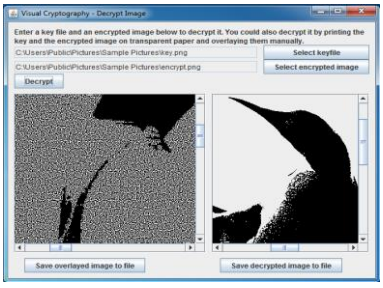

Fig. 7 Single Phase of Encryption

## V. CONCLUSION AND FUTURE ENHANCEMENTS

This paper proposed a new hierarchical visual cryptography scheme for gray scale image. By which a secret image is encrypted into two phases of levels. Shares generated by this scheme are gray and highly secured because original secret image is encrypted to maintain more secrecy. The hidden content is revealed only after overlaying the transparencies. In future, color share could also be generated by applying this algorithm on any of R, G and B components of color images. Instead of cutting an image into bits, it is also possible to consider it as a set of pixels, which are then available on different transparencies such that when all the transparencies are overlaid with the right orientation but in any order, the original code is visible. Each transparency will have white pixels, black pixels and blank spaces (where the pixels of other transparencies will be revealed). Further refinements and splitting of color pictures can be considered as possible developments.

## REFERENCES

[1] M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptogoly --- Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, 1-12,Springer-Verlag, Berlin,1995

[2] Pallavi V. Chavan, Dr.Mohammad Atique, "Design of HierarchicalVisual Cryptography", IEEE, 2013.

[3] Cheng-Chi Lee, Hong-Hao Chen, Hung-Ting Liu, Guo-Wei Chen, Chwei-Shyong Tsai, "A new visual cryptography with multi-level encoding", Elsevier/Journal of visual language and computing,2013.

[4] Shubhra Dixit, Deepak Kumar Jain and Ankita Saxena, " An Approach for Secret Sharing Using Randomised Visual Secret Sharing",IEEE,2014.

[5] Pallavi V. Chavan, Dr. Mohammad Atique,Dr. Latesh Malik,"Design and Implemantation of Hierarchical Visual Cryptography with Expansionless Shares", International Journal of Network Security & Its Applications,vol-6,2014.

[6] Pallavi V. Chavan, Dr. Mohammad Atique, Dr. Latesh Malik, "Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography", IEEE Conference on Elecrical, Electronics and Computer Science,2014.

[7] Trupti Patel, Rohit Srivastava, "Hierarchical Visual Cryptography For GrayScale Image", IC-GET 2016.

[8] Wen-Pinn Fang, Jia-Hao Hsu, Wei-chi Cheng, "Text-Based Visual Secret Sharing", IJCSNS vol.13 No.5,May 2013.

[9] Yawei Ren, Feng Liu, Teng Guo, Rongquan Feng, Dongdai Lin, "Cheating prevention visual cryptography scheme using Latin square", IET journals 2016.

[10] B Prasanalakshmi, A Kannammal, R Sridevi "Multimodal biometric cryptosystem involving face, fingerprint and palm vein" International Journal of Computer Science Issues, (2011)Vol.8, Issue.4, Pages.604