

# Color Extended Visual Cryptography for Visual Quality Improvement

Naga Subba Rao. G<sup>1</sup> Ravi Sekhara Reddy.V<sup>2</sup>

<sup>2</sup>Assistant Professor

<sup>1,2</sup>Department of Electronics & Communication Engineering

<sup>1,2</sup>LBRCE, Mylavaram-521230, India

**Abstract**— This paper presents a novel visual cryptography is a kind of digital image encryption, but it is different then compare to traditional cryptography techniques because of that it needs less complex time to decrypt the encrypted data. At present so most of the products are using this technology visual cryptography is split the secret image into number of random shares seperatly no information about secret image beyond the size of the secret image. This secured image can be reconstructed by grouping the all shares, here the main play role of this scheme is logical OR operation. This technique can be implemented encryption and decryption by rand shares of secret image into meaningful convert image. This paper presents study and performance analysis of visual cryptography technique on pixel expansion, various secret images shares generated.

**Key words:** VCS, Security, Computational complexity

## I. INTRODUCTION

With the rapid growth of network every one prefers network communication, in that the hackers utilize leak the secure information. So in that network secure data communication is one of the important tasks in real time scenario. For this scenario recently so many people are researched generally traditional cryptology is to avoid the problems but it needs complex computation time to decode in the receiver side. To overcome this time complexity and furthermore secure the data Shamir and Naor proposed a new visual cryptography scheme in 1994 with less mathematical calculations and it can restore the encrypted image by two shares to identify visual information. The starting stage this visual cryptography technique is used only on black and white images for confidential data is distorted. These distorted images are called shares, in that one can have cipher text and other can have key. Those hackers cant decrypt the secret data from single share, they must need two shares information then only get the secured information from that host image. Later they can extend the visual cryptography by using threshold visual cryptography scheme is splitted n number of transparent into secret data. Further in 1998 Wu and Chen proposed a new visual cryptography scheme. This scheme can overcome the drawbacks of the general visual cryptography algorithm that has to share images only can embed the confidential image into two shares.

This paper proposes to improve more than two shares of security deliver message. This secret information is more robust into three shares and improves security. This VCS with random shares the traditional or simply VCS.

## II. LITERATURE SURVEY

### A. VSC for general structure of multi pixel encoding with variable size

The multi-pixel encoding is a method of visual cryptography that it encodes more than one pixel for each iteration. In fact that encoding efficiency is still low, this paper presents a

multi pixel encoding scheme which can be encode variable pixel for each step. The size of the encoding at one step is equal to the number of consecutive same pixels met during scanning the secret image. This proposed work is well for general access without expansion of pixel size. This experimental results achieves high efficiency for good quality of overlapped images.

### B. Integration of Visual Cryptography and Watermarking

In this paper they discussed how to use digital watermarking technique for visual cryptography. Both of these two techniques are involved for hidden secret image. But their concepts are different for visual cryptography a set share binary images are used to protect the content of hidden image. In that watermarking technique the hidden image can involve a single halftone for preserving the quality of watermarked image. This paper shows both the watermarking and visual cryptography has merits.

### C. Improved Visual Cryptography Scheme for Data Hiding

This VCS is based on cryptography where n number of image are encoded in that way only the HVS can decrypt the secret data without any computations when all shares are preserved together. This VCS scheme is for hiding binary image into the grayscale image. These schemes are achieves lossless recovery and reduce the noise in the host image without adding external methods.

*D. Some of the Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:*

#### 1) RSA:

The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it — Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number,  $n$ , that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an  $n$  with roughly twice as many digits as the prime factors. The public key information includes  $n$  and a derivative of one of the factors of  $n$ ; an attacker cannot determine the prime factors of  $n$  (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure. (Some descriptions of PKC erroneously state that RSA's safety is due to the difficulty in *factoring* large prime numbers. In fact, large prime numbers, like small prime numbers, only have two factors!) The ability for computers to factor large numbers, and therefore attack schemes such as RSA, is rapidly improving and systems today can find the prime factors of numbers with more than 200 digits. Nevertheless, if a large number is created from two prime factors that are roughly the same size, there is no known

factorization algorithm that will solve the problem in a reasonable amount of time; a 2005 test to factor a 200-digit number took 1.5 years and over 50 years of compute time.

### III. PROPOSED SYSTEM

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table on the below we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.

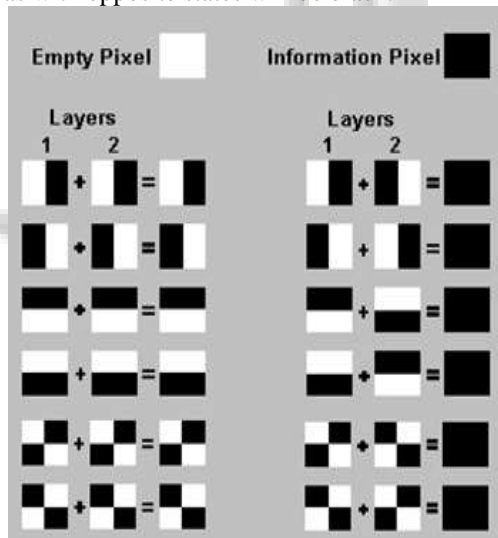


Fig1. Pixel division Table

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for

true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

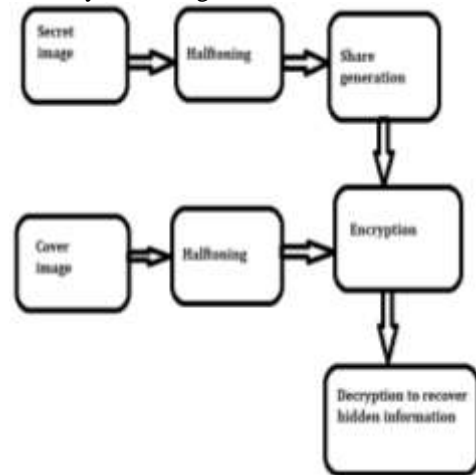


Fig.2. Block diagram

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as the two layers don't fall together in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

### IV. CONCLUSION

This paper presents a conventional visual secret sharing scheme it is usually to embed one confidential messages. It is also increased security. The proposed method not only increases the visual quality of recovered secret but also gives better results. It also improves the PSNR as compared to other methods. In future you can extend the conventional visual secret sharing scheme has been extended to encrypt three secret images.

### REFERENCES

- [1] InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on Image Processing, Vol. 20, No. 1, pp. 132-145, 2011
- [2] M. Naor and A. Shamir, "Visual cryptography", in Proc. EUROCRYPT, 1994, pp. 1-12.
- [3] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86-106, 1996.
- [4] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," ACM Theor. Comput. Sci., vol. 250, pp. 143-161, 2001.
- [5] Kai-Hui Lee and Pei-Ling Chiu "An Extended Visual Cryptography Algorithm for General Access Structures" in IEEE transactions on information forensics and security, vol. 7, no. 1, pp. 219-229, 2012
- [6] Rafael C. Gonzalez and Richard E. Woods "Digital Image Processing", Prentice-Hall, Inc., 2002.

- [7] Chris Solomon and Toby Breckon, “Fundamentals of Digital Image Processing”, John Wiley & Sons, Ltd, 2011.
- [8] Young-Chang Hou, “Visual cryptography for color images”, Pattern Recognition Society, Elsevier Science, pp. 1619-1629, 2003
- [9] Kai-Hui Lee and Pei-Ling Chiu, “Image Size Invariant Visual Cryptography for General Access Structures Subject to Display Quality Constraints”, IEEE transactions on image processing, vol. 22, no. 10, pp. 3830-3841, 2013.
- [10] C. Blundo, A. D. Santis, and M. Naor, “Visual cryptography for grey level images,” Inf. Process. Lett., vol. 75, no. 6, pp. 255–259, 2000.

