Visual Cryptography

Ganesh Bahalkar[1], Rupali Dhavale[2], Pranjal Ghule[3], Prerna Gangurde[4]
[1,2,3,4] Department of Information Technology
[1,2,3,4] MVP's, Karmaveer Adv. Baburao Ganpatrao Thakare College of Engineering, Nashik, Maharashtra, India.

Abstract- *Visual Cryptography is a special method of encryption to hide information in images in such a way that it can be deciphered by a human viewing system. The advantage of the visual encryption sharing scheme lies in its encryption process where without any complex cryptographic encryption data is removed using the Human Visual System. But the encryption process requires a cryptographic calculation to split the image into multiple parts let n. The k-n confidential sharing program is a special type of Visual Cryptographic strategy in which at least a group of shares from the n.*

In our paper we have proposed a new k-n privacy sharing system for color imagery where encryption is performed using the Random Number generator.

Keywords- Visual Cryptography, Secret Sharing, Random Number.

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (Image, text, etc.) to be encrypted in such way that decryption can be made into a visual human program without the help of computers.

Image is part of multimedia that people here. The smallest element of a digital image is pixel. In 32 digital imagery, each pixel has 32 pieces, divided into four parts, namely Alpha, Red, Green, and Blue; each has 8 pieces. The alpha part represents the level of reflection. If all the pieces of the Alpha part are '0', then the picture is completely clear.

The human viewing system acts as an OR function. When the two visible elements are put together, the final stack of objects will become clear. But if one of them is not visible, the last stack of objects will not be visible. As OR, 0 OR 0, you consider 0 as obvious as 1 OR 0 =1, 1 OR 1=1, view 1 as invisible.

In a K out of N visual cryptography scheme it is a type of cryptographic encryption in which a digital is divided into a number of shares by cryptographic calculation. In the process of writing by translating only the shares of K or more K can reveal the actual details (Here can create the first image). Below K the value of the shares cannot disclose the actual details.

In this paper we have developed an algorithm for dividing a digital color image into a number of shares where the minimum number of shares is sufficient to recreate the image. If K share numbers are taken the remaining (N-K) shares. In the figure if a specific pixel position is 1, then (N-K) + 1 the number of shares in that pixel position will be 1. For sites left in that pixel position it will be 0. A random number generator is used to identify those (N-K) + 1 share numbers.

II. RELATED WORK

Verheul and Tilborg were the first to process visual cryptography of color, in which the pixels in a secret image were taken from a given set of colors. Their model assumes that, when colored pixels are raised, one sees a special black color. With a c-color cryptography color scheme, pixel magnification m is c*3. Therefore in this model, there is an additional loss of resolution with the c element. Yang and Laih reduced the expansion of pixels to c*2 of Verheul and Tilborg. However, both schemes have only made senseless shares. Shyu has suggested a color encryption sharing scheme that works best with the increase in pixel log2 c*m where m pixel expansion of the binary system used. In most visual color schemes, when two pixels of the same color are highlighted, the resulting pixel becomes darker. Climato et al. check the color the black by highlighting the system, which should ensure that the secret reconstructed pixel is exactly the same color as the original. Kang et al. proposed the release of the N color Extended Visual Cryptography scheme using visual information pixel (VIP) to synchronize and distributed errors. VIP synchronization maintains positions of pixels that contain visual imagery in all color channels, the error distribution is used to create stocks so that sound presented by pre-set pixels is distributed to the neighbors when encrypted shares are made. This program can detect secret color messages with very low contrast and produce high quality colored stocks. However, the program also has a problem with pixel expansion. Monoth introduced three different ways to improve the brightness of cryptographic writing schemes-Additional Basis Matrix, complete reconstruction of White Pixel and complete reconstruction of Whit Pixels with additional basis matrix and applied to prepare non-compliance with question submission online with fingerprints. Teen and Lin have embraced Shamir-Lagrange’s secret photo-sharing process. Many researchers have suggested schemes for sharing confidential images based on sharing such as unreasonable shares, among hosted images; Ulutas et al. and sharing authenticity. Chen et al. created as secret method of images sharing based on Lagrange’s polynomial translation. N shadow images of a secret image are made by pressing, replacing, encoding and unraveling a secret image, each image of the shadow is hidden in a standard image so as not to attract the attention of the attacker.

III. PROPOSED SCHEME

The proposed scheme is mainly introduced for recovering the secret image without changing the color of the secret image.

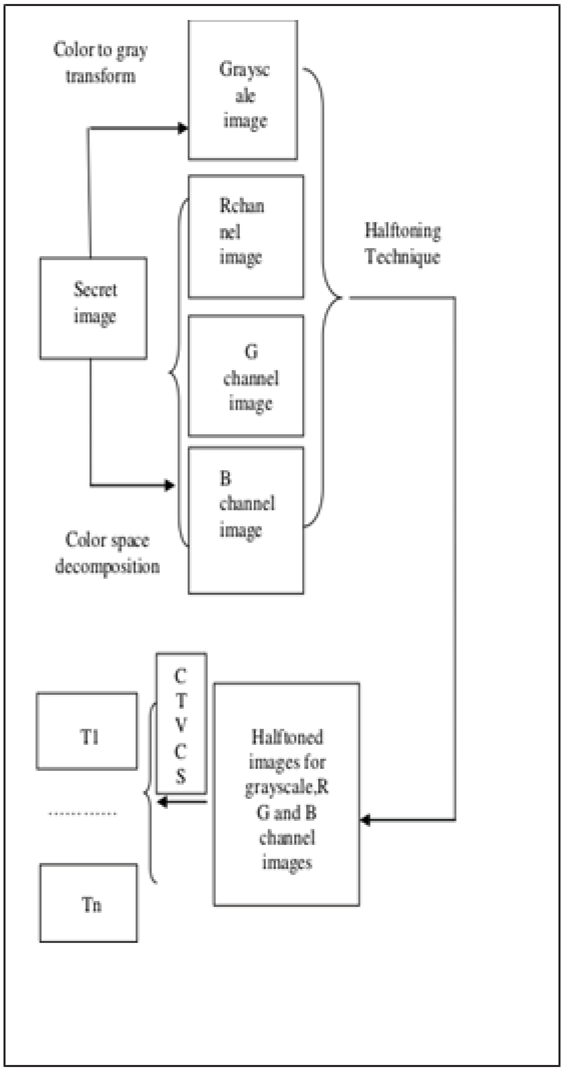

Fig.1 Color Transform Visual Cryptography

The motivation of the proposed color transfer visual cryptography scheme is to develop a technique for sharing a secret color image if each participant have only had black and white printers, fax machines, LCD displays device to output, transmit or display his/her transparency. However, the color information of the original secret images is required to be reconstructed during decryption.

The color transfer visual cryptography scheme is implemented by flattering the compressed color information into a single bit-plane with digital half toning and color decomposition. In this scheme, the secret image is decomposed into three color channels (R, G, B) and then the color channels are transformed into the grayscale version. Digital half toning is applied to these images for converting the greyscale and three color channel images into half tone versions.

Error diffusion half toning is the most widely used method. The principle of the error diffusion technique is that the error is diffused to the neighbors of the current processing pixel when half toning a continuous-tone image line by line sequentially. Next, four half tones of the greyscale, R, G, B channels are integrated encrypted with a modified (k, n) Visual Cryptography Scheme. In this way, the color information is embedded into the transparencies during the processing. In the decoding stage, the inverse procedures are executed.

Fig. 1 shows the color transfer visual cryptography scheme for encryption. In the figure, the secret image is the color image. The color image is transformed into a greyscale image. The secret color image is also decomposed into three different channel images called R, G, and B channel images. The four images (Grayscale, R, G, B channel images) are converted into half tone images by using the error diffusion half toning technique. After the conversion of half tone images, the color transfer visual cryptography scheme is applied to these images. Then the transparencies are produced and encrypted. These images are recovered by stacking these shares at the receiver’s side. The decrypted image has the exact color of the secret color image.

IV. ADVANTAGES

1) Decryption algorithm is not required. So a person unknown to cryptography can decrypt message.
2) Simple to implement.
3) Lower computational cost since the secret message is recognized only by human eyes and not cryptographically computed.
4) The main advantages of visual cryptography scheme over normal cryptography technique is that it does not requires complex computations at the receiver side. Here proposes

a visual cryptography scheme for preserving the colour of the secret image for avoiding the disadvantages of the existing schemes.

5) The data computation process at the receiver is almost absent except for the stacking of the shares, which immediately reveals the secret input. Hence, is more computational efficient than other cryptographic techniques.

V. FUTURE SCOPE

Visual cryptography is used to make data secure. Here the actual information is divided into multiple shares sent through various communications channels from sender to recipient. The attacker therefore has little chance of getting all the information. But still it is not so secure. This can be made safer by introducing a balanced key to the encryption process and decryption process.

Using the key, the image is first encrypted and then divided into multiple shares. If a criminal finds the number of shares k / we cannot encrypt them if the key is unknown to him. By key, letter or number combination can be used. The high-bit switch makes the images more blurry, so the key can be applied to the top bits of each pixel.

A small image can also be used as a key. Let the image size w1*h1 be taken as the key where w1< w and h1< h. The first image is separated by w1*h1 blocks. For each block, (w1, h1) pixel is inserted with (w1, h1) pixel keyword. The reversal process will be used to remove the disassembly. Encryption can be done by left or right shift of bits of each pixel of the original image.

VI. CONCLUSION

In this this paper we have suggested the process of sharing k-n privacy but in color images. When dividing the image into stocks we used a random number generator, which is a new method that is not available yet. This method requires very little statistical calculation compared to other existing cryptography techniques visible in color images. This method only tests ‘1’ in a small area and divides that ‘1’ into (n-k+1) shares using random numbers. In most of our test results, each assignment shows very little or no information about the first image in the human eye.

But the biggest problem with the algorithm lies in its number of loops. At n=6,k=5 and 32 bit pixels with 50% ‘1’, the required loop operating number is 32. In n=6, k=4 and other similar cases, the required loop function value is 48. n=6, k=3 and other similar conditions, the required loop operations number is 64. Apart from this regression the algorithm produces better results compared to other existing algorithms.

REFERENCES

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

[2] Rashmitha, K., Mr G. Bhaskar, and Mr Bramha Reddy., “A Secure Viusal Cryptography for Color Images,” International Journal of Engineering Research and Development, 2012.

[3] Verheul E. and Tilborg H., “Construction and Properties of K out of N Visual Secret Sharing Schemes,” Designs, Codes and Cryptography, vol. 11, no. 2, pp. 179-197, 1997.

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