Enhance Visual Cryptography of Image

[1]Abhishek Dhoke, [2]Piyush Pande, [3]Tanushree Kosarkar, [4]Prof. Ganesh Padole

[1,2,3] Research Scholar, [4]Assistant Professor

Rajiv Gandhi College of engineering and Research

Nagpur, India

Abstract: Image Cryptography is a special encryption technique to hide information in images, which divide secret image into multiple layers. Each layer holds some information. The receiver aligns the layers and the secret information is revealed by human vision without any computation. The proposed algorithm is for color image that presents a system which takes four pictures as an input and generates three images which correspond to input pictures. The decoding requires only selecting some subset of these images, making transparencies of them, and putting them on top of each other, so the forth picture is reconstructed by output images onto putting them together. The reconstructed image achieved in same size with original secret image.

Index term: Image cryptography, secret sharing, primitive color

I. INTRODUCTION

I m a g e cryptography is a popular solution for image encryption. The secret sharing concepts, the encryption procedure encrypts a secret image into the shares which are noise-like secure images which can be transmitted or distributed over a communication channel. The properties of the to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional Image 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 Image Cryptography Scheme. The simplest Image Cryptography Scheme is given by the idea of a secret image consists of a collection of black and white pixels where each pixel is treated independently [2]. There are many algorithm to encrypt the image in another image, but a few of them have been in Image cryptography for color image. In this paper, the different approach has been produced for the computations and any knowledge of cryptography [1]. Image cryptography for color image, the proposed algorithm splits a secret image into three shares based on three primitive color components. This paper gives a review of the literature and research in this field and it concerns with the main fundamental concept to understand the idea of Image cryptography color image and theoretical foundation for each algorithm.

II. IMAGE CRYPTOGRAPHY

The original clear text is revealed by placing the transparency with the key over the page with the cipher, even though each one of them is indistinguishable from random noise. The model for Image secret sharing is as

follows. There is a secret picture to be shared among n participants. The picture is divided into n shares such that if any m transparencies are placed together, the picture becomes visible. If fewer than t r a n s p a r e n c i e s are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately [1]. There are some researches that deal with Image cryptography for color images. In this section, we will explore several representative works over the years. [3] Discussed the Image cryptography scheme which reconstructs a message with two colors, by arranging the colored or transparent sub pixels. The approach by [5] is basically similar to Koga's. Both approaches assign a color to a sub pixel at a certain position, which means that displaying m colors uses m−1 sub pixels. The resulting pixels contain one colored sub pixel and the rest of the sub pixels are black. Therefore the more colors are used, the worse the contrast of the images becomes significantly. Their approaches cannot be applied to the extended Image cryptography, either. Rijmen and Preneel talked about enabling multicolor with relatively less sub pixels (24 colors with m = 4)[6]. However each sheets must contain color random images, which means applying this approach to the extended Image cryptography is impossible.[7]

Figure 1: Image cryptography system Encryption

In Image cryptography system the pixels of the image to be encrypted can be applied to the image in different manner. There is a set of n participants, and the secret image is divided and encoded into n shadow images called shares Each participant encrypted by one share, k out of n participants are needed to combine shares and see secret image, some time k-1 of shares can not reveals information about secret image.

The technology makes use of the human vision system to perform the OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind. For example, a block of 2×2 pixels will be viewed as a gray-like dot as the two black pixels and the two nearby white pixels are averaged out. If

we print the 2×2 pixel blocks shown in Fig. 2 separately onto two transparencies and superimpose them. This effect is equivalent to performing a pixel-wise the secret recovery process can easily be carried out by superimposing a number of shares (i.e. transparencies) without requiring any computation [8].

Figure 2: Image cryptography system Decryption

III. IMPLEMENTATION

Every single pixel in secret image is splited into sub pixels , that can still perceived them as one pixel by Human vision system. The security of each share depends crucially on the color composition of the original secret image. To recovering a secret image, it is required that the cover image should at least be able to determine the shape or pattern of the original secret image, which is able to determine the boundary between two distinct color regions in the image. In this paper, for the problem of interest here, assuming an input 24-bit bitmap color image which each 3-byte sequence in the bitmap array represents the relative intensities of red, green, and blue, respectively for image sized 256*256 RGB pixel for hiding Original image.

In the following, the steps of the proposed algorithm and illustrate it using an example where the original secret image is a 24-bit color original image shown in Fig.3. The encryption process consists of determining the arrangements of transparent sub pixels on each sheet according to the pixel transparencies,

Figure 3: Original secret image

The proposed algorithm first decomposes the original image into three primitive- color images under the subtractive model namely Red, Green and Blue. The three primitive color components of the Original image, where each image has 256 levels of the corresponding primitive color, and each pixel represented by three bytes. Converting to R,G, B, where R,G, B {0- 255}. For each pixel of the C primitive $P_{i,j}$ will be store it in the other image for reducing the $P_{i,j}$ value by holding ¼ $p_{i,j}$ the color of a pixel in the original secret image in terms of primitive red, green and blue with reducing value,

respectively. Selecting the cove image to encrypt on it the secret image depends on minimum difference between the value of pixel, there are three primitive color, therefore we need three cover image to generate three share . In this step, three shares, namely a, b and c shares are generated each share contains apart of secret image. To generate these shares, the R, G and B the reduction primitive-color images of the original secret image are read in pixel by pixel and mixing(OR operation) together with ¾ pixel of cover image For example if the pixel value of primitive color equal 00000011 and the value of the cover image is 01101100 the output pixel will be 01101111 by OR operation. So, each share (a, b, and c) hold part a primitive color for secret image, for example share (a) which is baby image holds R primitive color , share (b) flower image holds G primitive part and share(c) fish image hold B primitive color , selecting of the cover image depending on minimum differences between pixel in cover image and primitive color in secret image. To share a secret pixel with color (R,G, B) in cover image depending on the value of threshold for selection the proper image. It is found that the shares reveal the information about the secret image. To recover the secret original baboon image it is necessary to   removing the unwanted color in each share by the operation 255.

IV. EXPERIMENTAL RESULT

In this paper, the number of pixel in the decoded image is same as in the original secret image because the pixel p not expanded. The size of secrete image must be smaller or equal to the cover images. After testing many different images from different colors and in resolution it was observed that the proposed algorithm could not take dark image significantly with high contrast and which then generate the unclear share, and they appears as images corrupted with large amount of noisy and it will be easy to detect.

We have added some processing elements after recovering the secret image to change the quality of color to be clearer and give the similar original view. This is to be done after removing unwanted color from the share and before stacker the shares together. The way of this processing is changing pixel value to $P_{i,j}$ multiplying by 4 to get full value from 255, so for secret image will reveal the secret completely in shares in case of with the previous processing.

The way of reduction in original pixel and subtractions of the original pixel with previous shares pixel give more sensitive result and with better color quality. Our results suggest that the security of the image depends critically on the color composition of the secret image and distribution of the original secret image.

V. CONCLUSION

In this paper, provided a security Image cryptography   for 24-bit bitmap color image. After splitting the image to the number of the shares and applying some method according to the color mixture groups we identified the adversary may find out some useful information such as the shape or pattern of the original secret image. The number of images are tested to hiding the   part secret image and it is found that the image with color near to the primitive Red, Green and Blue. In particular, it can find out the shape of the original secret image with each share and the original secret image is color image and the adversary has acquired three of the R, G and B

shares. and each share may only be able to retrieve partial information of the original secret image.

Our results suggest that the security of the scheme depends critically on the color composition and distribution of the original secret image.

REFERENCES

[1] Talal Mousa Alkharobi, Aleem Khalid 2003. New Algorithm For Halftone Image Cryptography,
Alvi King Fahd University of Pet. & Min. Dhahran.

[2] JIM CAI 2003. A Short Survey on Image Cryptography. Schemes, www.wisdom.weizmann.ac.il /naor/PUZZLES /Image.html.

[3] Nakajima, M. and Yamaguchi, Y.2002. Extended Image Cryptography for Natural Images, WSCG02, 303.

[4] M. Naor and A. Shamir, 1996. Image cryptography ii: Improving the contrast via the cover base. Theory of Cryptography Library, (96-07).

[5] Hiroki Koga and Hirosuke Yamamoto, 1998. Proposal of a lattice-based Image secret sharing scheme for color and gray-scale images. IEICE

[6] E.R. Vaheul and H.C.A. van Tilbong, 1997. Constructions And properties of k out of n visual secret sharing scheme.

[7] V. Rijman and B. Preneel, 1996. Efficient colour visual Encryption or shared colors of Benetton.