Proposing Progressive Visual Cryptography Scheme for Color Images by Halftone Technique

Debashis Sanki[1], Dr. Nisarg Gandhewar[2]

[1] Research Scholar, Department of Computer Science and Engineering, Dr. A.P.J Abdul Kalam University, Indore, M.P.

[2] Research Guide, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, M.P.

Article Info
Volume 83
Page Number: 378-386
Publication Issue:
November /December 2020

Article History
Article Received :*25 October 2020*
Revised: *22 November 2020*
Accepted: *10 December 2020*
Publication: *31 December 2020*

Abstract

In visual cryptography, a secret picture is encoded into n bits of noise, similar to sharing, and this is a significant data encoding method. The hidden picture can be decrypted by the naked eye if there are more than k shares stacked out of n shares; this cannot be done if there are less than k shares accessible. Using the halftoning approach, a novel progressive visual cryptography (PVC) scheme for colour pictures is proposed in this study. A chromatic picture is first reduced to three monochromatic images in red, blue, and green tones. This is the first step. The halftone approach is used to convert these three pictures into binary images. It is the unexpanded VC method that reveals the secret image sharing in binary pictures.

Keywords: Visual Cryptography, Halftone, Progressive, Watermarking, Color image

I. INTRODUCTION

For information storage, transport, and retrieval, the world now relies on the internet. For this reason, the internet is flooded with multimedia content. Military maps and commercial identifications are only two examples of sensitive information that might be exchanged over the internet without permission. While using hidden photos, security concerns must be taken into account because hackers may use a weak link in the communication network to get access to information they desire. Various picture secret sharing techniques have been created to deal with the security issues of secret photos.

Noar and Shamir proposed visual cryptography in 1994. Encryption of information in visual form is possible using the visual system alone, without the use of a computer, thanks to visual cryptography. The decryption procedure can be simplified by using visual cryptography, which removes the need for complicated computations. Visual cryptography is particularly beneficial because of its minimal computational burden.

One of the most powerful visual secret-sharing schemes is visual cryptography, in which a secret picture is divided into two or more noise-like shares and dispersed across a group of participants (or shadow images). The original hidden image will be disclosed without the need of mechanical means like a computer when the shares on transparencies are layered together. The Human Visual System can be used to decrypt information. According to Naor and Shamir's approach to visual cryptography, a picture may be encoded into many shares (printed on transparencies) by expanding each pixel m times.

II. CONCEPT OF PROGRESSIVE VISUAL CRYPTOGRAPHY

In order to ensure the best possible secret recovery and reconstruction, Progressive Visual Cryptography takes this into account. Computational effort is required in many cases to achieve a complete reconstruction of the secret. Progressive Visual Cryptography" (PVC) arose as a novel sharing idea that gradually disclosed the secret picture as the number of shares increased.

The threshold approach is used to retrieve sensitive information in VC. When more than k shares are piled together, the human eye can decipher the encrypted information. Nothing private can be seen if less than k shares are accessible. the substance of sensitive information gets increasingly comprehensive with each further exchange.

III. PROPOSED SCHEME OF METHODOLOGY

Using an unexpanded share mechanism and a digital watermark, the suggested colour image sharing strategy creates a progressive visual cryptography. You may achieve meaningful shares through watermarking. The steps in this plan are as follows:

At the encryption stage

1. It is possible to create three monochrome pictures from a chromatic image using the primary colors red, blue, and green.
2. The halftoning approach is used to convert these three pictures into binary images.
3. Making the photos for sharing.
4. A cover image is placed on top of each sharing.

At the decryption stage

1. The important shares are divided into their original shares.

2. In order to make it easier for investors, these shares are divided into three colour channels.

3. Combining red, blue, and green colour channels to produce grayscale pictures.

4. The colorful hidden picture is created by combining three grayscale photographs.

A chromatic picture is first reduced to three monochromatic images in red, green and blue tones. This is the first step in the process. These three pictures are then reduced to binary images using the halftone approach.

This is a way for displaying a black-and-white image with black-and-white spots. Figure 1 illustrates the fundamentals of halftone printing. The blacker specks a picture has, the more it will resemble the original grey image. Figure 1 (b) is the closest to the grey image when the other two binary images, depicted in Figures 1 (c) and Figures 1 (d), are constructed.

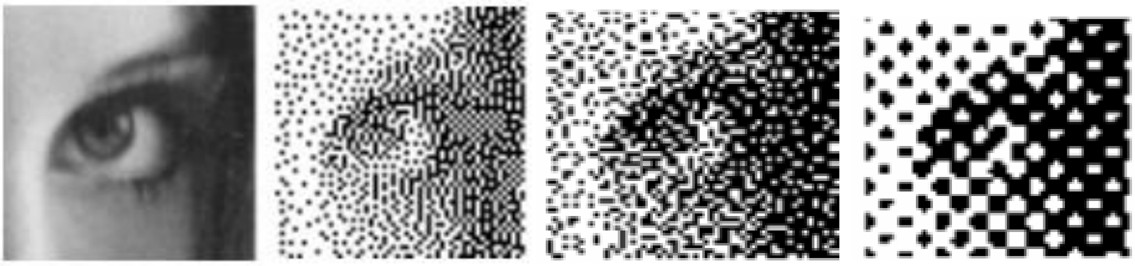
The Floyd-Steinberg Algorithm is used to generate the halftone pictures in this work. The grey values of an 8-bit grayscale picture range from 0 (black) to 255 (white) (white).

Letting b=0,

w=255,

t= int [(b+w)/2] =128.

If g is the image's grey value, then P (x, y) is its position, and the difference between e and g is e. then the algorithm is referred to as the Floyd Steinberg Algorithm



(a) Gray image **(b) Binary** **(c) Binary image 2** **(d) Binary**

Figure 1: Basic principle of halftone technique

```
If      g > t then
        Print white;
        e=g-w;
        Else Print black;
        e=g-b;
        (3/8 × e) is added to P (x+1, y);
        (3/8 × e) is added to P (x, y+1);
        (1/4 × e) is added to P (x+1, y+1);
End if
```

A point with the grey value of 130, for example, should be gray-pointed in an image. Due to the dynamic nature of the image, the values of nearby pixels are likely to be close to 130, as well as grey, and the surrounding area.

A white point is printed on the new picture if the number 130 is greater than the number 128, according to the algorithm. It's a little more than half a dozen. Although the neighboring pixel's value is near to 0, the adjacent pixel's value is -46 (-125 multiplied by 3/8), which makes it dark. Next, e becomes positive, and the neighboring pixel changes colour to white, resulting in a grey pixel following a black one. The new picture has a white pixel if the old one was black. Suppose that the grey value of a point is 250, and e = -5, and the next pixel is white in the grey picture. This validates the algorithm's accuracy.

The progressive VC approach developed by Young Chang Hou and Zen-Yu Quan is then utilised to produce n shares of the hidden picture. N shares are generated for each of the three monochromatic photos using this procedure. n shares are generated per image.

Afterward, we may pick any three colours from which to build n coloured shares using the procedure below.

Create two n × n matrices, C^0 and C^1, to represent the secret image's sharing matrix for white and black pixels. There is a row for each sharing mechanism, and each column reflects the value allocated to each participant in the C^0 or C^1 matrix (0 is for white, 1 is for black).

The first row of matrix C^0 has the value 1, whereas the other rows have the value 0. There's an exception to this rule, however: Matrix C^1 is a symmetrical diagonal matrix, which means that each of its members is equal to 1. The secret image's white and black pixels are randomly distributed over the pixels on the shares, so each share's pixel has only a 1/n chance of being black.

To generate shares, you'll need a random number between 1 and n. It's important to note that when distributing white pixels in a picture, the values of C0's lth row vector are used for each share. This implies that the first value of [C^0 (l, 1)] is distributed to share 1, then the second value [C^0 (l, 2)] is sent to share 2, and so on. C1 is used in the same manner as sharing a white pixel to share a black pixel.

The design's detailed algorithm is shown in the next section. Then, we may combine three separate shares of varying hues to create an infinite number of colors. It is then watermarked using a basic watermarking method for each channel, i.e. red, blue and green. " Thus, each share is generated and then overlaid with a cover picture to provide a meaningful sharing. Following is an explanation of the watermarking algorithm.

Two N×N Secret Sharing Matrices

$$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{R\times R} \qquad C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{R\times R}$$

Progressive and unexpanded VC algorithm

Input: A W × H halftone secret image P where p (i, j) ϵ P

Output: n shares, Sm=1, 2, …., and n

Process:

```
1) Generate sharing matrices, C0 and C1
2) For each pixel p (i, j), 1 ≤ i ≤ W, 1 ≤ j ≤ H
3) Randomly choose a value l, range from 1 to n
4) For m=1, 2, and n
    • If the pixel p (i, j) = 0 (white), the pixel value
        Sm (i, j) = C0 (l, m)
    • If the pixel p (i, j) = 1 (black), the pixel value
        Sm (i, j) = C1 (l, m)
```

Decryption involves obtaining the original shares from the significant ones. For each watermarked sharing, take a pixel measurement and convert it to a height and width. There are only two ways to obtain the black-and-white secret picture shares: either by setting each watermarked share pixel's lower-left bit to 0 or by setting it to 1. Each colour channel must go through this process. After that, the shares are divided into three colour channels, and the identical colour channels are combined to produce grey scale pictures of red, blue, and green, in order of decreasing contrast. To begin with, we can only see a skeleton of the concealed image (in grey scale), but as the number of shares being piled grows, we obtain a clearer and clearer picture. The colorful hidden image is created by combining the three grayscale photos from the three different channels.

The fundamental difficulties of leakage of secret information, pixel expansion, and poor quality of recovered photos are all addressed by progressive visual cryptography with unexpanded shares, as is the issue of colour images. When the procedure couldn't create significant shares, watermarking the shares may be used as a solution. This concept's goal is to make it easier to conceal natural photographs in various significant ways, so that recovered images with high contrast and good security may be guaranteed. Fingerprint and facial templates may be protected and authenticated using this method.

Watermarking Algorithm

Input: n secret image shares, n cover images

Output: n watermarked shares

Process: Do for each secret image share

```
a. Read respective cover image
b. Do for each pixel
    i.  If share pixel is black
            • Set LSB of cover image pixel to 1
    ii. ii. If share pixel is white
            • Set LSB of cover image pixel to 0
```

IV. RESULTS AND DISCUSSION

As illustrated in Figure 2, the experiment's input picture is composed of 512 384 pixels in size (a).

Figure 2 shows the halftone image created using the halftone approach (b).

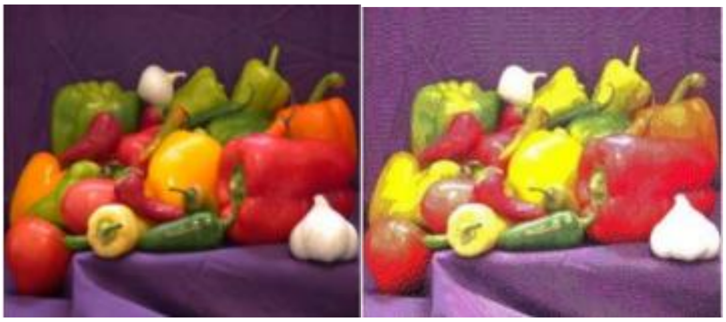
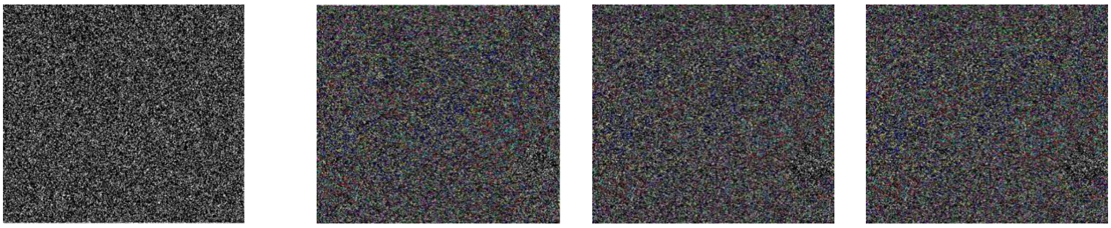


Figure 2: (a) Secret image (b) Halftone image

This approach uses Young-Chang Hou and Zen Yu Quan's progressive VC method to produce n shares of the same colour as a secret monochromatic image, and then we may pick three distinct colors of shares to assemble n coloured shares from those three. In this case, we're looking at n=4. Figure 3 (a), (b), (c) and (d) show the four coloured shares S1, S2, S3 and S4 created by combining three distinct colors from the halftone picture.



S1 **S2** **S3** **S4**

Figure 3: Colored shares

LSB watermarking is used to incorporate the shares into various cover pictures once they have been created. Figures 4 and 5 illustrate the watermarked shares and their corresponding cover pictures. It's now in the decryption process for these watermarked shares that were transmitted. From the valuable shares, the original shares are culled. After that, the shares are divided into three colour channels, and the identical colour channels are combined to produce grey scale pictures of red, blue, and green, in order of decreasing contrast. There is no hidden picture if there is just one share R1. Figure 6 (b) results from stacking two shares.

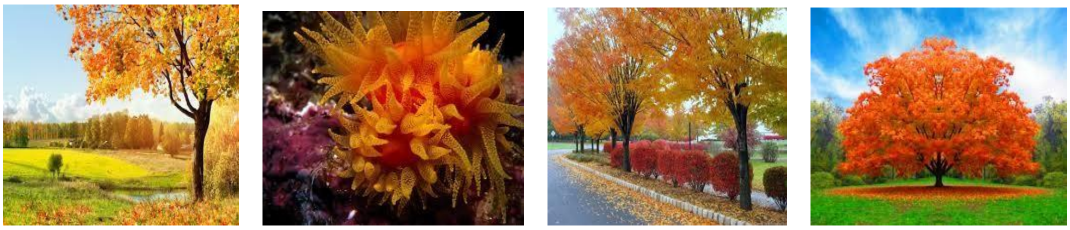


Figure 4: Cover images

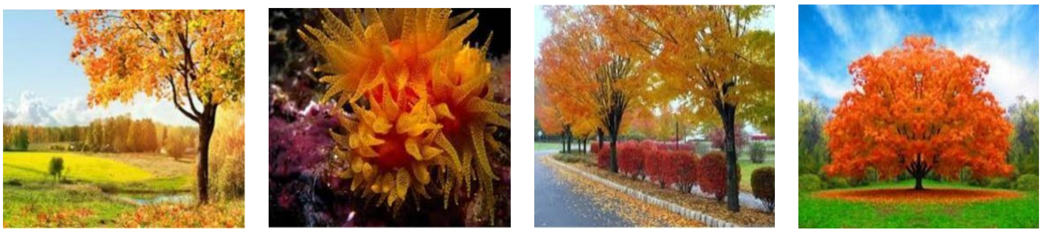
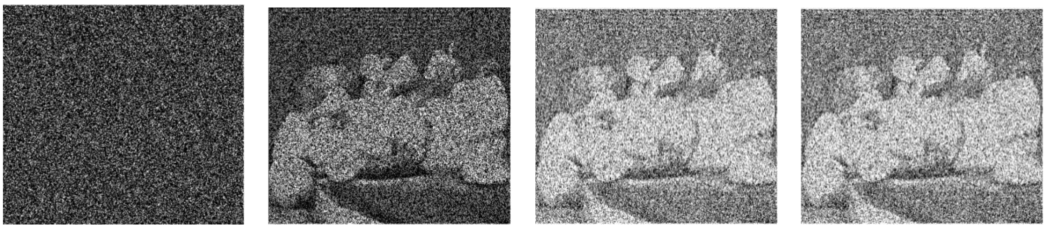


Figure 5: Watermarked shares

Figure 6 shows the grayscale picture of red if there are four shares (d). Figures 7 (a) and 7 (b) depict the progression of grey scale pictures of green and blue, respectively. To create the colorful hidden image displayed in Figure 8, these three channels' grey scale images were merged.



(a) R1 **(b) R1+R2** **(c) R1+R2+R3** **(d) R1+R2+R3+R4**

Figure 6: Gray scale images of red.

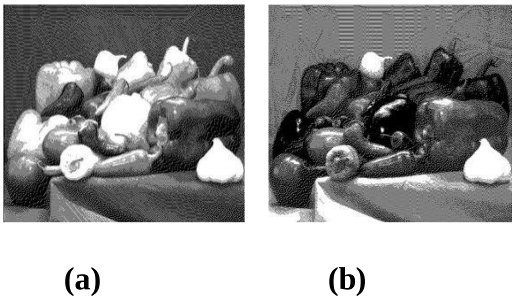


Figure 7: (a) Gray scale image of green. (b) Gray scale image of blue.

The peak signal-to-noise ratio (PSNR) is expressed in decibels (dB). Only data represented in terms of bits per sample or bits per pixel has any use for the PSNR. Integers 0 to 255, for example, are included in a picture with 8 bits per pixel.

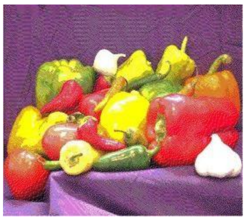


Figure 8: Reconstructed image

The following equation defines the PSNR:

$$PSNR = 20\log_{10}\frac{2^B - 1}{\sqrt{MSE}}$$

where MSE represents the mean square error and B represents the bits per sample.

When comparing data with an approximation, it is important to know how much of a discrepancy there is between what you have and what you have estimated.

Mean Square Error (MSE) is the squared norm of the difference between a picture and an approximation, Y, multiplied by the number of images in the image:

$$\frac{\|X - Y\|^2}{N}$$

Calculating the PSNR from the halftone and reconstructed images yields an infinite value. So we may infer that both images are of equal quality, and that the half-toned image can be correctly recreated during the decryption step of the algorithm.

We obtain a PSNR of 51.1427 when comparing the cover picture with the watermarked image. There is little difference in the cover image's quality when hidden shares are inserted into it.

V. CONCLUSION

A watermarking approach is used to produce significant shares of a new PVC scheme for colour photos without any pixel enlargement based on the halftoning technique.

We can infer from the results that the halftone image can be perfectly decrypted. In addition, the quality of the cover picture is largely unaffected by inserting the hidden shares, and they appear to be similar from a visual standpoint.

REFERENCES: -

1. Xiaotian Wu and Wei Sun (2015) Extended Capabilities for XOR-Based Visual Cryptography.
2. C.-N. Yang and D.-S. Wang, “Property analysis of XOR-based visual cryptography,” IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 2,pp. 189–197, Feb. 2014
3. Jithi, P.V.; Nair, A.T., "Progressive visual cryptography with watermarking for meaningful shares," International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Vol., No., pp.394, 401, 22-23 March 2013.
4. Hou Y., Quan Z., Tsai C., and Tseng A., “Block based Progressive Visual Secret Sharing,” Information Sciences, vol. 233, pp. 290-304, 2013.
5. Tu S. and Hsu C., “A Joint Ownership Protection Scheme for Digital Images based on Visual Cryptography,” The International Arab Journal of Information Technology, vol. 9, no. 3, pp. 276- 283, 2012.
6. Aarti, Harsh K. Verma and Pushpendra K. Rajput, "Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based (k, n)- VCS," International Journal of Computer Applications (09758887) Vol. 46, No. 9, May 2012.
7. Young-Chang Hou and Zen-Yu Quan, “Progressive Visual Cryptography with Unexpanded Shares,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, No.11, November 2011.
8. X. Wu and W. Sun, “Random grid-based visual secret sharing for general access structures with cheat-preventing ability,” J. Syst. Softw., vol. 85,no. 5, pp. 1119–1134, May 2011
9. F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38,Mar. 2010
10. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics, Security, Vol. 4, No. 3, pp. 383–396, Sep. 2009.
11. R.-Z. Wang, “Region incrementing visual cryptography,” IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009
12. D. S. Tsai, T. H. Chen, and G. Horng, “On generating meaningful shares in visual secret sharing scheme, “The Imaging Science Journal, Vol.56, 2008, pp. 49-55.
13. W. P. Fang, “Friendly progressive visual secret sharing,” Pattern Recognition, Vol. 41, 2008, pp.1410 – 1414.
14. Tu S. and Hou Y., “Design of Visual Cryptographic Methods with Smooth-looking Decoded Images of Invariant size for Gray Level Images,” Imaging Science Journal, vol. 55, no. 2, pp. 90-101, 2007.
15. W. P. Fang and J.C. Lin, “Progressive viewing and sharing of sensitive images,” Pattern Recognition and Image Analysis, Vol. 16, No. 4, 2006, pp. 632-636.
16. Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., Vol. 15, No. 8, pp.2441-2453, Aug 2006.