ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 11, May 2013

A Probabilistic Model of Visual Cryptography Using Halftoned Technique for Color Image

Rajesh Kumar Rai[1], Swati Yadav [2]
1Professor, Electronics Department, NIIST, RGTU, Bhopal (M.P.) India
[2]M. Tech Scholar, NIIST, RGTU, Bhopal (M.P.) India

Abstract - Visual Cryptography is a special type of encryption technique which is used to hide the information and data in images. In this technique the decryption process is done without any complex cryptographic computation. The encrypted data is decrypted using Human Visual System (HVS). This is the benefit of the visual secret sharing scheme. The encryption technique requires a cryptographic computation to divide the image into a number of parts or we can call it shares. We divide the image into n number of shares. In this paper we proposed a new secret sharing VC scheme for taking two images one is black and white image with size of 127x261 and other is color image with size of 196x92.In contrast with the previous color visual cryptography schemes, the proposed one enables to share images without pixel expansion and to detect a forgery as the color of the message is kept secret. In order to correctly print the colors on the media and to increase the security of the scheme, we use spectral models developed for color reproduction describing printed colors from an optical point of view.

***Index terms:* Visual Cryptography, Probabilistic Scheme, Halftone Technique, Zig Zag Scanning.**

I. INTRODUCTION

VISUAL cryptography (VC) is a branch of secret sharing. In the VC scheme, a secret image is encoded into transparencies, and the content of each transparency is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques. In general, a -threshold VC scheme has the following properties: The stacking of any out of those VC generated transparencies can reveal the secret by visual perception, but the stacking of any or fewer number of transparencies cannot retrieve any information other than the size of the secret image. Naor and Shamir [1] proposed a –threshold VC scheme based on basis matrices, and the model had been further studied and extended. The related works include the VC schemes based on probabilistic models [2]–[4], general access structures [5], [6], VC over halftone images [7], [8], VC for color images [9], cheating in VC [10], [11], the general formula of VC schemes [12], and region incrementing VC [13]. Contrast is one of the important task for this vc scheme, so in this paper contrast of image is good and here is no pixel expansion is done. Generally, the stacking revelation of the secret with higher contrast represents the better visual quality, and therefore the stacking secret with high contrast is the goal of pursuit in VC designs. Naor and Shamir [1] define a contrast formula which has been widely used in many studies. Based on the definition.

II. IMPLEMENTATION

A. VCscheme

Definition 1. A solution to the t out of n visual secret sharing scheme consists of two collections of n × m Boolean matrices M0 and M1. To share a white pixel, the associate randomly chooses one of the matrices in M0, and to share a black pixel, the associate randomly chooses one of the matrices in M1. The chosen matrix defines the color of the m sub pixels in each one of the n transparencies. The solution is considered valid if the following three conditions are met [2]:

Contrast

1) For S in M0 (WHITE): $H(V) < d- \alpha m$

2) For S in M1 (BLACK): $H(V) \geq d$

Security

1) For any subset $\{ i1, i2, . . . iq\}$ of $\{1, 2, . . . n\}$ with $q < k$, the two collections of $q \times m$ $(1\leq q \leq k)$ matrices, formed by restricting $n \times m$ matrices in C0 and C1 to any q rows, are Generally, we suppose the basis matrices M0 and M1 are used to encode white and black pixels, respectively. They have the same dimension $n \times m$. suppose the secret image is SI with $L \times H$ pixels and the n share are S1, S2… Sn, respectively. In gray-scale or chromatic images, the white pixel usually means blank and black pixel means non-blank.

B. Scanning Mode is Zig-Zag scanning

its scanning order is shown in Fig. It is very different from two scanning modes that is Row-by-Row and Colomn-by-Colomn scanninf mode at most situations the next pixel to be scanned is adjacent to the current one with both different row and different column. Therefore, to some extend this scanning mode can be suitable for more kinds of images. It is noticeable that an image is not always square. When it is rectangular, the zigzag scanning will still work well. For a comprehensive consideration, our proposed scheme will adopt zigzag scanning mode to scan the original image.

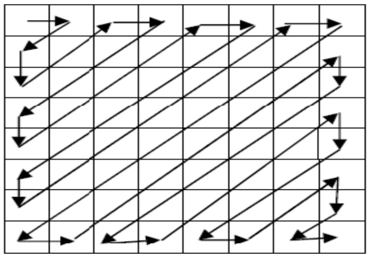


Fig 1. Zigzag scanning order

C.Encryption Algorithm

1. Divide the pixels of the image into N number of sub pixels or we can say divide the data sets into N sub data sets.
2. Now the original data set can be constructed from any K data sets out of N data sets.
3. The K-1 data sets can represent the information of the original data set. Write K data sets out of N data sets.
4. A pixel P is split into two sub pixels in each of the two shares.
5. If P is white, then a coin is tossed. Then the pixel P is encrypted as two sub pixels in each of the two shares. Every pixel is encrypted using a new coin toss.
6. If pixel P is black, then we get both sub pixels black when we superimpose the two shares;
7. If P is white, then we get one sub pixel black and one sub pixel white when we superimpose the two shares.
8. Thus, we can say that the reconstructed pixel has a grey level of 1 if P is black and a grey level of 1/2 if P is white. There will be a loss of 50% contrast in the reconstructed image, but it will be still visible.

The decryption algorithm decrypts the shares into the original image. The decryption algorithm is as follows:

D.Decryption Algorithm

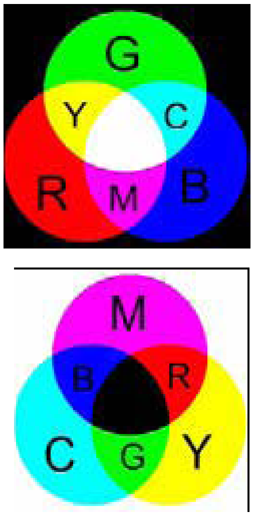
1. Read the Encrypted Image called Img
2. Read the image Pixel by pixel called Px(i,j) is the current pixel
3. Decompose the pixels in n sub block relative to the Encryption algorithm.
4. Perform the Decoding on each sub block
5. Marge the sub blocks Extract 8 valid bits
6. Reform the image from these pixels
7. Return the result image.

III THE PROPOSED SCHEME APPLIED TO CHROMATIC IMAGE

A chromatic image is usually composed of three dimensional parts. Each dimensional part is a gray-scale image. However, like the traditional Naor-Shammir [1] scheme, most VSS schemes are initially designed for binary black-and-white images. In order to work for grayscale or chromatic images, many researches try to design respective basis matrices for different colors on a secret image. In this paper, we introduce a technology called halftoning, which can transform a continuous-tone image into a binary one, to make the proposed scheme smoothly work for gray-scale and chromatic images.

A. The Model of Color

A color model is a way to specify colors. It is usually represented as a three-dimensional space. There are many kinds of color model; the most common models are RGB and CMY shown in Fig. In terms of RGB model, each color is mixed with red, green, and blue, which are the three primary colors of light. This model is commonly used for on-screen display. Mixtures of pure red, pure green and pure blue light produce white light. Therefore, RGB model is also called additive model. On the other hand, CMY model is called subtractive model. For CMY model, each color is mixed with cyan, magenta, and yellow, which are the three primary colors of pigments. This model is commonly used for color printing. Generally speaking, the more colors of pigments are mixed, the more wavelengths of light are absorbed. The mixtures of pure cyan, pure magenta and pure yellow absorb all wavelengths of light and hence produce black. In fact, the RGB model and CMY model are mutually complementary, which can be easily learnt from Fig. . For example, the mixture of pure magenta and pure yellow in CMY model produces pure red in RGB model; the mixture of pure green and pure blue produces pure cyan in CMY model.



(a) RGB color model (b) CMY color model

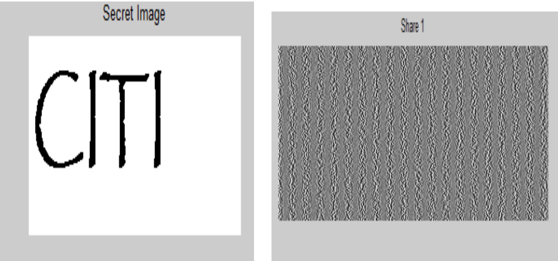
Flow chart of encryption is shown in Appendix.

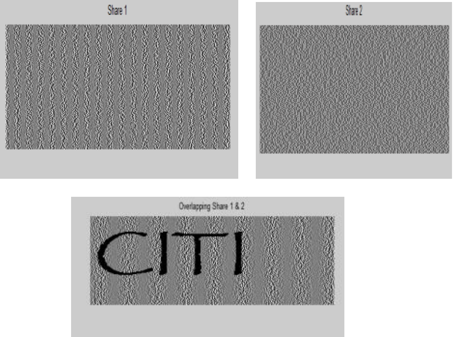
B. Halftoning

The main idea of halftoning is to utilize the density of printed dots to simulate the grey scale of pixels. For human eyes, the denser the dots are, the darker the image is; on the contrary, the sparser the dots are, the lighter the image is. For example, if the black dot densities of two areas with same size are 90% and 50% respectively, the human visual system can perceive the difference between them: the former is darker than the latter and the latter lighter than the former. Therefore, we can learn that the black dot density can simulate the gray-scale value of an area. Just by dominating the black dot density of an area, halfoning transforms a continuous-tone image into a binary one.

IV RESULT

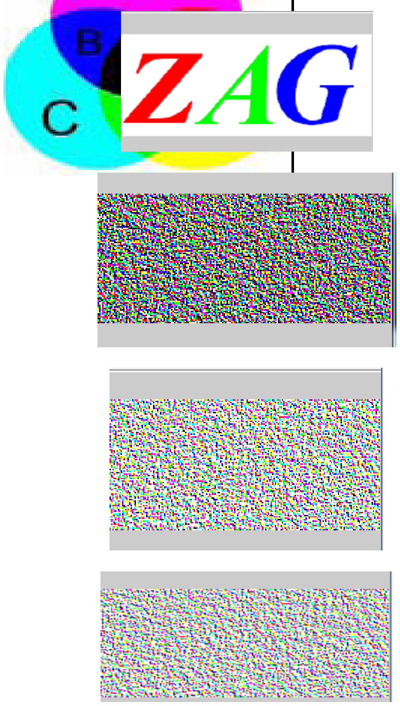
This the (2,2) VC





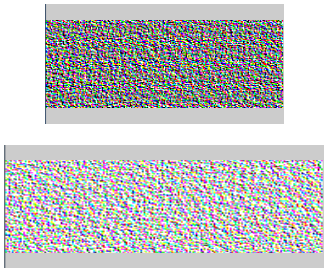
Binary Input image Share1

Share2 Hidden output image



Color input image Share1

Share2 Share3



Share4 Result of color image

V. CONCLUSION

We have proposed a VC scheme with flexible value of . From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of VC with unlimited. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic model is adopted in the scheme.

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography,” in Proc. Advances in Cryptography (EUROCRYPT’94), 1995, vol. 950, LNCS, pp. 1–12.

[2] C. N. Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognition. Lett., vol. 25, pp. 481–494, Mar. 2004.

[3] S. J. Lin, S. K. Chen, and J. C. Lin, “Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion,” J. Vis. Common. Image Represent. vol. 21, pp. 900–916, Nov. 2010.

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[5] 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.

[6] 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.

[7] Z. 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.

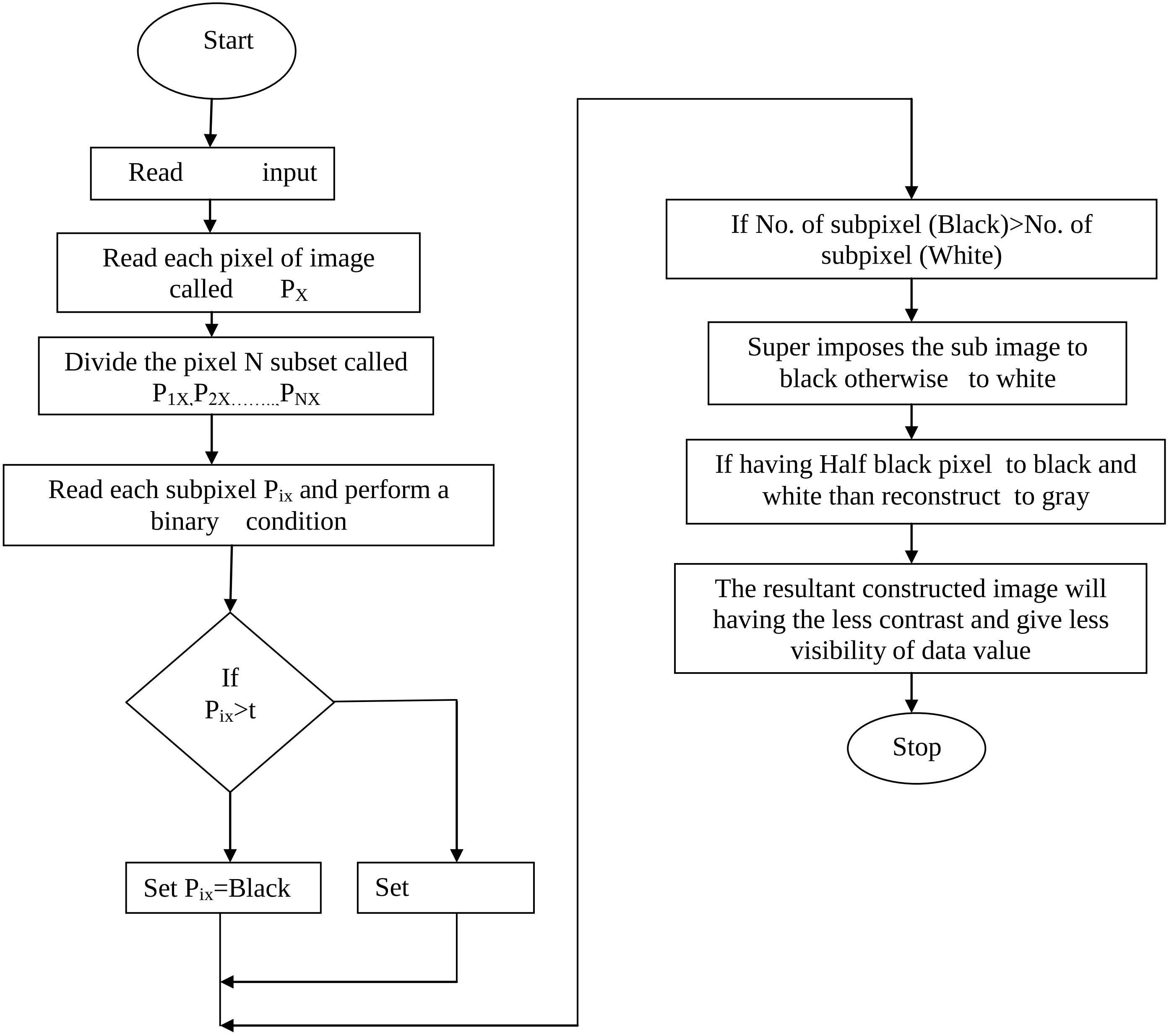
AUTHOR BIOGRAPHY

Swati Yadav received B.tech. From P.I.R.M.E.Collage JNTU Hyderabad (A.P.) in 2008 and currently pursuing M.Tech. in Digital Communication from NIIST, affiliated to RGTU, Bhopal. His area of interests is Digital Communication, Image Processing and WIMAX.

Rajesh Kumar Rai received M. E. (Elect) Degree with specialization in Digital Techniques & Instrumentation from S.G.S.I.T.S. Indore in June 2008. His Research interests are Image Processing, Embedded System & Communication. He is Ph.D scholar in JJT University, Rajasthan. He has worked as a Assistant Professor & Head of Electronics Department in Siddhant College of Engineering, Pune, affiliated to University of Pune, Pune (India).Presently he is associated with NIIST, RGTU, Bhopal as a Associate professor in Department of Electronics & Communication. Life time member of IEEE & ISTE.Published 8 international papers.

APPENDIX

Flow chart of encryption


Start
Read input
Read each pixel of image called P_X
Divide the pixel N subset called P_{1X}, P_{2X}……..P_{NX}
Read each subpixel P_{ix} and perform a binary condition
If $P_{ix}>t$
Set P_{ix}=Black
Set
If No. of subpixel (Black)>No. of subpixel (White)
Super imposes the sub image to black otherwise to white
If having Half black pixel to black and white than reconstruct to gray
The resultant constructed image will having the less contrast and give less visibility of data value
Stop