International Conference on Inventive Systems and Control (ICISC 2019)
IEEE Xplore Part Number: CFP19J06-ART; ISBN: 978-1-5386-3950-4

Visual Cryptography for colour images using multilevel thresholding

Pooja Kashyap
Computer Science and Engineering Department
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
poojakashyap.2193@gmail.com

Renuka A.
Computer Science and Engineering Department
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, India
renuka.prabhu@manipal.edu

***Abstract*—Visual Cryptography Scheme, is even known as VCS. It is actually a cryptography method to encrypt an image by dividing it in parts called shares, where decryption is performed using Human Visual System (HVS), only by overlapping all these shares. The image to be encrypted is called a secret image. Visual Cryptography can be used for binary image, grayscale image as well as colour image. This paper implements visual cryptography technique for colour images, by using multilevel thresholding so as to enhance the obtained quality contrast of reconstructed image.**

Keywords—Visual cryptography, secret image, share image, multilevel thresholding

1. INTRODUCTION

Needless to say, how important digital security has become nowadays, to transfer sensitive data online or offline, leading to the demand of data security higher than ever, in the history of data security. This is because the different ways in which the unintended recipients can now actually steal data or even change the original data, for that matter. Doing all this without even letting the original sender know any of it, is quite dangerous.

To help our data stay secured, from such threats, different fields of science like steganography, cryptography, visual cryptography and others have evolved. Coming to visual cryptography, which was introduced basically to solve a very important problem of the time, that was the problem of secret sharing, implying the sharing of secret data.

Visual Cryptography was first introduced by Moni Naor and Adi Shamir in 1994 [1]. It was this time that the authors proposed a visual secret sharing scheme, where a secret binary image is taken as input and it is then divided into n different shares.

The decryption of this is done only after overlapping all these shares in a way that a person with all the n shares only, could decrypt the image, while someone with anything less than the original n shares can retrieve no information about the original image, whatsoever [1].

Each share can even be printed on a different transparency, and overlapping these transparencies, would give back the original image. However, the aim of any data hiding technique is to transfer a message securely, in a way that the secret message isn't available to an unintended observer, no matter what.

2. RELATED WORK

Moni Naor, Adi Shamir [1] proposed a new cryptography scheme in his paper called Visual cryptography, where this scheme was also extended to a visual variant k out of n secret sharing scheme, where the recipient receives each of the n shares created, however superimposing any k out of these n shares or transparencies in that case will give back the original image. Stacking any less than k shares will give no information about the secret image, thereby making this scheme perfectly secure. However, the images used by authors were black and white (binary) image.

The images exchanged on internet nowadays are highly colour images. Visual cryptography had to be extended to be used further for colour images so that more and more information is transmitted, and more use of visual cryptography schemes can be involved, with data security.

This was achieved when Young Chang Hou proposed three different algorithms for visual cryptography of colour images [2]. The techniques of colour decomposition and halftoning methods are used to get the shares that when stacked together give a contrast reduction upto 25%. However, in another algorithm given by him, with the increased number of shares, the contrast reduction becomes 50% of the original image.

The methods proposed here [2], does even retain all the pros of a black and white visual cryptography, as stated in [1], that actually exploits HVS to decrypt the image, with no cryptographic computation at all, but it is also completely backward compatible with all the results already achieved in the work proposed in here [1]. It can even be applied to encode grayscale images.

This was the first paper that proposed methods that would exploit colour decomposing and technique of halftones to generate visual cryptograms. The next point to be noted is that, the shares formed are meaningless shares and therefore it might attract a hacker's attention. The shares being meaningless imply that they are noisy and noisy shares attract hacker's attention unintentionally.

To avoid such shares, there have been many researches based on the methods that create meaningful shares. S.Srividhya[3] implemented and proposed a modification on Two in One Image Secret sharing scheme, where meaningful shares are created and to make sure that no hacker could introduce any fake shares, an authentication image is shared along with secret image.

Li Shundong, LI Jiliang, Wang Daoshun[4] implemented Region Incrementing Visual Cryptography Scheme (RIVCS) where the secrets of multiple secrecy regions can be revealed by human visual system and in RIVCS, since different regions have different contrast. However to achieve same contrast throughout, integer linear programming was done.

Hao Luo, Hua Chen, Yongheng Shang, Zhenfei Zhao, Yanhua Zhang[5] proposed the first colour transfer visual cryptography scheme. It is unique because it develops a secret colour image sharing scheme that can be easily used by monochrome printers or fax machines, since the shares produced in this scheme are still binary images. The scheme proposed requires a key for encryption and decryption of message, which is why it is not a perfectly secured threshold scheme. This security problem was then later solved by Ching-Nung Yang, Tzu-Chia Tung, Fu-Heng Wu, Zhili Zhou when he proposed a (k,n)-CTVCS that needs no key for encoding or decoding and thereby provided perfect security [6]. Different uses of visual cryptography even involves image password based security system as proposed in a work mentioned [7]

3. PROPOSED WORK

The methodology proposed in this paper is the visual cryptography scheme that uses colour decomposition and multilayer halftoning technique to construct shares based on the halftones obtained. The method first decomposes an image into its primary colour components based on the RGB colour model. At the end of this step, three different colour components of a colour image, are obtained. For each of these three colour components obtained, multilevel halftoning is employed, individually.

Based on the three separate halftones obtained for each colour component, three shares are built in a way that share 1 has red and green component details of the secret image, share 2 contains the green and blue component details and share 3 has the red and blue component details of the image, in a way that these three shares when stacked together will reveal the original image.

The following has also been explained in the form of three modules: colour decomposition, halftoning and building share images, in Figure 3.1 and Figure 3.2.

MODULE 1:
Color Decomposition Technique
In this module, a secret image of size MxN is taken as input and it is decomposed into its constituting primary colour components. The algorithm uses RGB colour model for colour decomposition, and therefore the obtained 3 colour component images are red, green and blue components of the secret image, and denoted by R, G, B respectively.

MODULE 2:
Halftone Technique:

Multilevel halftoning is used to convert every individual colour component image, obtained in module 1, into its respective halftoned image, such that red halftone image RH, for red colour component, GH for green colour component and BH denoting blue halftone image, which is obtained by multilevel halftoning of blue colour component image. The multilevel halftoning, in this paper is done considering 5 different levels of pixel values.

MODULE 3:
Building Shares:

Based on each possible pixel value of these 3 halftone images, taken together as triplet (RHij, GHij ,BHij), where subscript 'ij' denotes the pixel positioned at i^{th} row and j^{th} column of the mentioned halftoned image, there are $125(5^3)$ possible combinations of the triplet (RHij, GHij, BHij), because the level in multilevel halftoning is taken as 5. For each of the possible 125 combinations, shares are built accordingly. The share building technique is shown in Figure 3.3, where based on each pixel triplet of the red, green and blue halftones (RHij, GHij, BHij), three different shares are built.

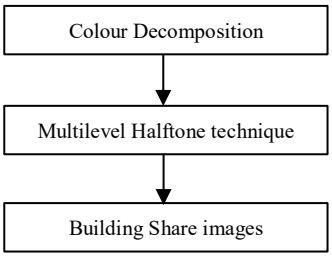

Fig. 3.1. Modules flow diagram for encryption

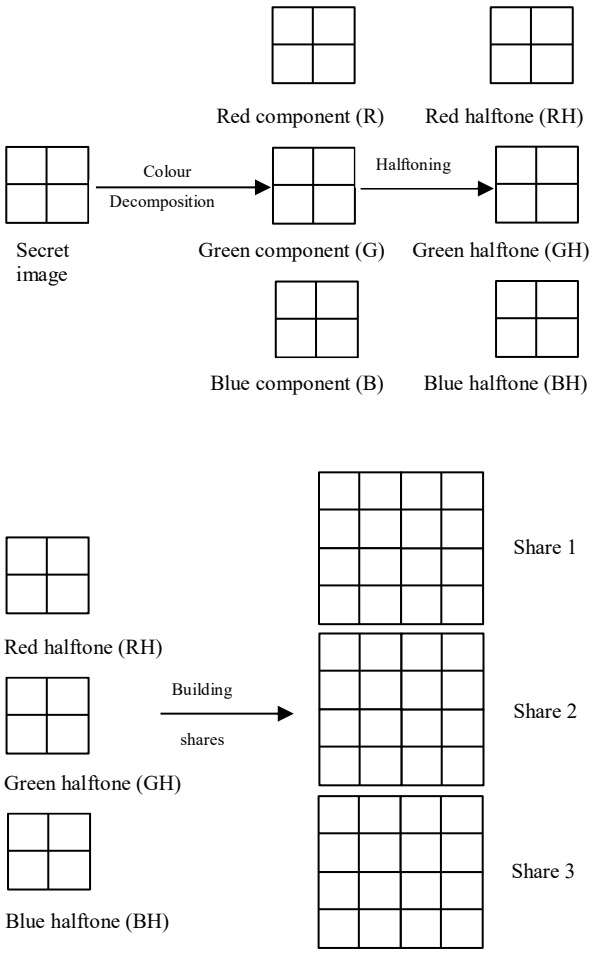

Fig. 3.2. Method overview for encryption

Now the shares are built in a way that Share1 gets red and green halftone details of the image, Share2 will have the green and blue halftone details and Share3 has the information for red and blue halftone of the image.

For each of the pixel in three halftone images obtained, the shares will be built, based on the 125 possible pixel triplet combinations of those three halftone images (5 threshold values for each colour plane). For each of the possible 125 triplets of pixel coordinate RH_{ij}, GH_{ij} and BH_{ij} of the red, green and blue halftone images respectively, four pixels are taken in Share1, Share2 and Share3 each, to build corresponding shares for that particular pixel triplet of original secret image.

Based on the value of the pixels (RH_{ij}, GH_{ij}, BH_{ij}) for a given pixel located at coordinate value (i, j) in images RH, GH and BH, the corresponding pixels in Share1 will have any two pixels of values RH_{ij}, GH_{ij} out of its four pixels, Share2 has its any two pixels with values GH_{ij}, BH_{ij} out of four pixels and Share3 has two pixels of values RH_{ij}, BH_{ij} out of its corresponding four pixels and the remaining two pixels of these four pixels will be black for each of the shares.

The position of black pixels in any of these shares, should be chosen in a way that the black pixels of any one share coincides with only the black pixels of the rest of two shares, in case shares are overlapped. This process is carried out for every pixel location (i, j) present in the halftone images. It can be noted that the size of the share images is increased to twice the size of original image, which is the size of shares will be 2Mx2N.

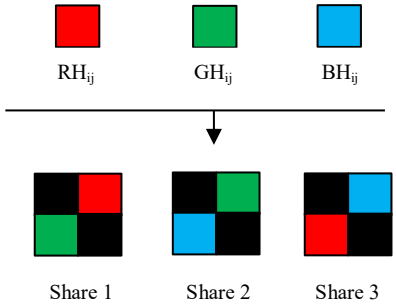

Fig. 3.3. Share building

4. Result Analysis

The execution of the entire project was achieved with MATLAB R_2018a, Windows 8 operating system and a 64-Bit 2.30GHz Intel Core i5 processor computer system. The method was implemented for colour images to give the results as obtained below.

In VCS, when a secret image is decomposed into its corresponding shares, no single share, on its own, should be capable of revealing any information about the secret image.

For the secret image shown in Figure 4.1, its three colour halftone images are shown in Figure 4.2, Figure 4.3 and Figure 4.4. Corresponding shares, Share1, Share2, Share3, then obtained are shown in Figure 4.5, Figure 4.6, Figure 4.7 respectively. It can be easily seen that no share reveals any information about the secret image, which proves that the secrecy of the shares is so well intact.

On overlapping these shares, the decrypted image can be retrieved, as shown in Figure 4.8.

Fig. 4.1. Secret Image

Fig. 4.2. Red halftone image

Fig. 4.3. Green halftone image

Fig. 4.4. Blue halftone image

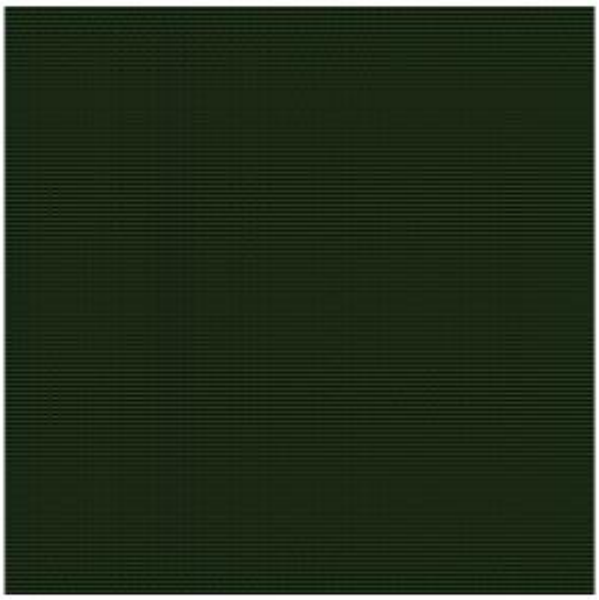

Fig. 4.5. Share 1

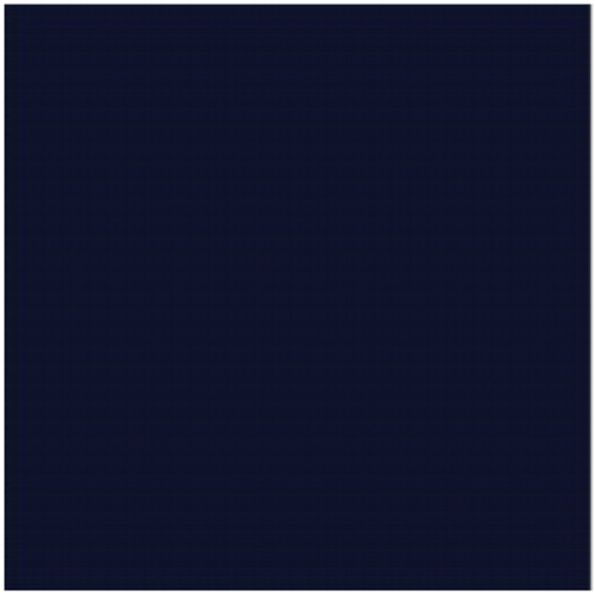

Fig. 4.6. Share 2

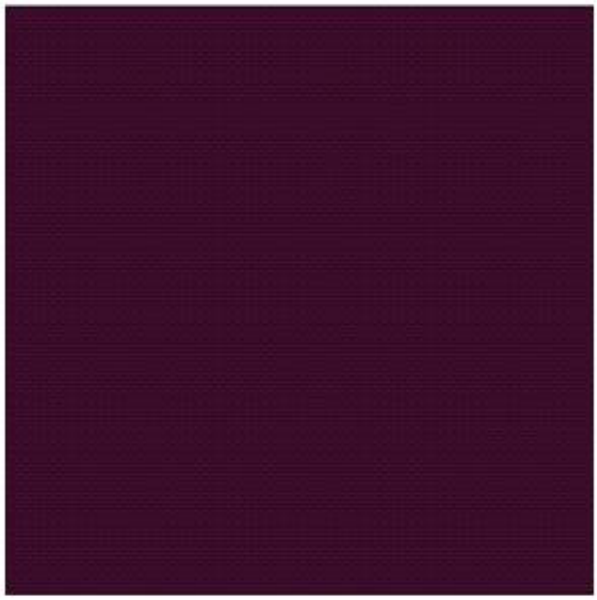

Fig. 4.7. Share 3

Fig. 4.8. Decrypted image obtained on stacking three shares

The decrypted image obtained, has so much more colour details in the image that is not possible without multilevel thresholding. This is actually because of the number of levels in multilevel thresholding present, in the algorithm proposed.

The earlier techniques that use binary halftoning to build shares can bear only 2 shades of any colour(red, green and blue), shade 1 being the colour with its maximum intensity value,255 and shade 2 being its lowest intensity value which is 0.Thus 2 shades of 3 primary colour channels(RGB or CMY), leading to a total of 5 levels of information only, of which 3 will be the three different colours with their full intensity, fourth is white(presence of all colours) and fifth being black(absence of any colour).

Contrasting to which, using multilevel thresholding with 5 levels, the number of levels of information is actually increased to 14, in which there are 4 different shades for each of the three primary colours of the chosen model and one black and one white, thus highly contributing to the colour details of the original image. The reason being multilevel halftoning.

The encryption and decryption of the algorithm does experience a pixel expansion of 4 because for each pixel in the secret image, there are 4 pixels in each of the shares. In a similar way, the algorithm can work well for grayscale images, as well. It can be even put to good use in case to send an ATM pin code for joint account, so that the password is revealed only after all the joint account holders turn up and put their shares together.

To make sure, this is possible, the algorithm was executed for a number image, as well. The secret pin code image is displayed in Figure 4.9 and then its three shares in Figure 4.10, Figure 4.11, Figure 4.12. The decrypted image for same is also given in Figure 4.13.

Coming to the secrecy of the shares, once again, we demonstrate it for the secret number image given in Figure 4.9 and the first two shares already shown in Figure 4.10 and Figure 4.11. On assuming, that an intruder gets hold of these two shares and however tries overlapping them with any other random share, built by him in Figure 4.14, just so to retrieve the original image.

For these three shares, out of which only two are genuine and the third is just a random share, we get a reconstructed image, shown in Figure 4.15, obtained on overlapping Encrypted Share1, Encrypted Share2 and the random share in Figure 4.14.

The image in Figure 4.15 clearly shows that no secret information about the original image (in Figure 4.9), whatsoever, has been revealed. Thus we can see, the secrecy of shares is maintained to utmost level, as the reconstructed image would reveal the original image only when all the three shares overlapped, are genuine.

Fig. 4.9. Secret number image

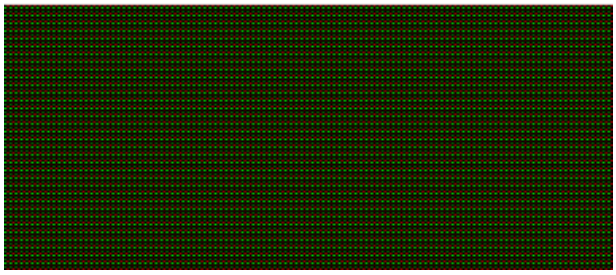

Figure 4.10: Encrypted Share1

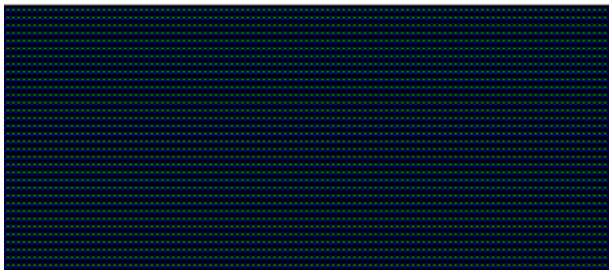

Figure 4.11: Encrypted Share2

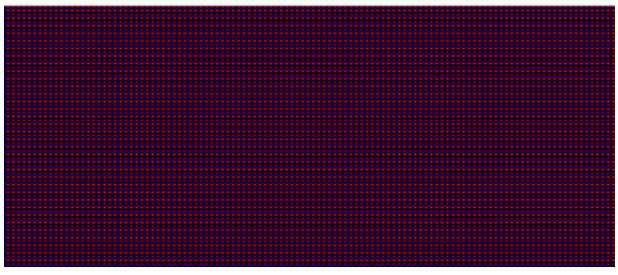

Figure 4.12: Encrypted Share3

Figure 4.13: Decrypted Image

Figure 4.14: Random share

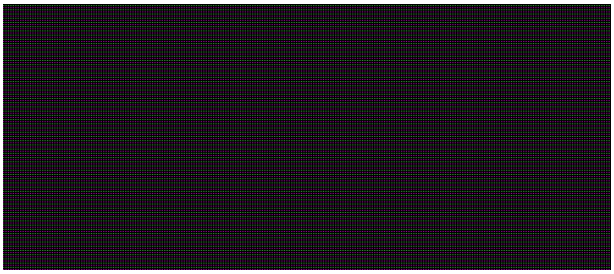

Figure 4.15: Reconstructed image made of Share1, Share2 and Random share

5. CONCLUSION

We can conclude that multilevel halftoning technique is better than binary halftoning as it lets the reconstructed image have more shades of colours, or more levels of information than what is attained with binary halftoning.

To be specific, a 5-level multilevel halftoning achieves 15 information levels, which would only further increase with the increase in levels of halftoning, as compared to the always fixed 5 levels, in binary halftoning. Therefore, giving a more detailed reconstructed image by losing less information of the image. More colour details are therefore retained in the reconstructed image.

One pixel of the secret image is given by four pixels in each of the share images, therefore this method observes a pixel expansion of 4 units (2 pixels lengthwise and 2 pixels breadthwise) which results in a two times longer and two times broader reconstructed image.

The shares are very random thus the data security is maintained to the utmost level. Stacking of any of these two shares will reveal no information at all unless all the three shares are stacked to get back the reconstructed image that reveals the original secret image.

The reconstructed image has a contrast reduction of 50%. This can be concluded because the contrast of a reconstructed image is given as the difference between number of pixels used to denote a black pixel and a colored pixel in the reconstructed image [8]. Here in order to denote a colored pixel, in a reconstructed image, no. of block used out of 4 are 2. To denote a black pixel, however 4 out of 4 blocks are used. Therefore a difference of 2 blocks, to denote a colored and a black pixel separately from a total of 4 blocks. Thereby, making the colour contrast to 50% of the original image.

6. REFERENCES

[1] Moni Naor and Adi Shamir " A Visual Cryptography" in proceedings of Advances in cryptology , EUROCRYPT 94, Lecture notes in computer science ,1994.

[2] Young-Chang Hou " Visual Cryptography for colour images" Department of information Management ,National Central University, Jung Li, Taiwan 320, ROC Received 6 June 2002, accepted 26 August 2002.

[3] S.Srividhya, R.Satishkumar, Gnanou Florence Sudha "Implementation of TiOISSS with meaningful shadows and with an additional authentication image" J.Vis.Commun.Image R., accepted 8 March 2016.

[4] Li Shundong, LI Jiliang,WANG Daoshun "Region Incrementing Visual Cryptography with same contrast" Chinese Journal of Electronics ,Vol 25, No. 4,July 2016.

[5] Hao Luo, Hua Chen, Yongheng Shang, Zhenfei Zhao, Yanhua Zhang "Color Transfer in Visual Cryptography" Measurement 51(2014), 81-90, 27 January,2014.

[6] Yang CN, Tung TC, Wu FH, Zhou Z, "Color transfer visual cryptography with perfect security" Measurement. 2017 Jan 1;95:480-93.

[7] Pandya, R., Patel, J. Patel, B. Patel "Image Password Based Security System" International Conference on Current Research Trends in Engineering and Technology, 2018

[8] Young Chang Hou, Zen Yu Quan and Hsin-Yin Liao "New design for friendly visual cryptography" International Journal of Information and Electronics Engineering, Vol. 5, No. 1, Jan 2015.