International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Utilizing the RGB Color Model and Halftone Technique for Color Segregation in Visual Cryptography

Sk Asfaq Ahamed[1], Indranil Sarkar[2], MD Altabuddin Molla[3], Sandip Roy[4], Rajesh Bose[5]

[1]JIS University, Department of Computer Science and Engineering, Agarpara, Kolkata700109, India
Email: *skasfaqahamed786[at]gmail.com*

[2]Guru Nanak Institute of Technology, Department of Computer Applications, Sodepur, Kolkata 700114, India
Email: *indra.nil2004[at]gmail.com*

[3]Elitte College of Engineering, Department of Computer Science and Engineering, Sodepur, Kolkata700113, India
Email: *altabuddin123[at]gmail.com*

[4]JIS University, Department of Computer Science and Engineering, Agarpara, Kolkata700109, India
Email: *sandiproy8686[at]gmail.com*

[5]JIS University, Department of Computer Science and Engineering, Agarpara, Kolkata700109, India
Email: *bose.raj00028[at]gmail.com*

Abstract: ***When the right key image is utilised, a specific encryption method called visual cryptography can be used to conceal information in images so that it can be decoded by the human eye. This experiment describes a halftone-based, covert visual cryptography system for colour graphics. A colour picture is first divided in to three monochrome picture with red, green, && blue tones. Second, using the halftone approach, these three images are converted to binary images. Finally, the sharing images are obtained using the conventional binary secret sharing approach. This plan offers a more effective technique to conceal natural photographs in various ways. Furthermore, the size of the shares remains constant regardless of how many colours are visible in the hidden image.***

Keywords: Color image, halftone approach, visual cryptography, secret sharing

1. Introduction

Aesthetic cryptography is a cryptographic method that makes it possible to encrypt visual data (images, text, etc.) in a method that eliminates the need for computers and enables manual decryption by the human visual system. Since Networking technologies have substantially improved, a lot of information can now be conveniently and quickly delivered over the Internet. The transmission procedure is also severely hampered by the security issue. The data may, for instance, be intercepted whenever a transmission is in progress. With this approach to create a technique for cryptography that can encode any picture in any common format so that the encrypted picture, whether seen without the aid of a device or when the image is being sent and intercepted by someone with malicious intent [1]-[3].

The Visual Cryptography Scheme (VCS) was first introduced by Naor and Shamir in 1994 as a means of secure photo sharing. The purpose of VCS is to randomly break a picture in to a number of piece that, when combined, only reveal the actual hidden picture's size. Simply superimposing a set amount of shares will reconstruct the picture, since it just contains black and white pixels [4]-[5]. Here the illustration utilising a black-and-white version of Lena that has been dithered (Figure 1).

(a) (b)

Figure 1:(a) Original Hidden Picture (b) Dithered

The 2-of-2 Naor-Shamir test graphical encryption method yields two shares (printed on transparencies), and when examined independently, neither share reveals anything about the original image. Only after both shares are acquired and superimposed is it recoverable [6]-[7]. The two shares are depicted in Figure2 along with their superimposition. Please be advised that the images have a 4x size enlargement.

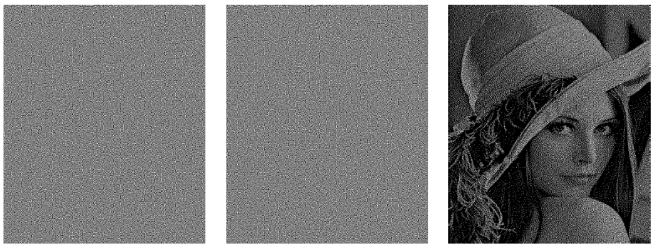


Figure 2: Superimposing the shares on top of two shares

Utilizing the human vision system, the technology performs the overlay of the shares' pixels subjected to an OR logical operation. whenever the pixels are sufficiently tiny and closely spaced, the colours of adjacent pixels will be averaged out by the human visual system, creating a smooth mental image for the viewer. As an illustration, the two adjacent white pixels and the two black dots in the 2, 2 cell block below will be averaged out to appear as a grey dot. When printing the 2 by 2 pixel in Figure 3 individually on to two layers, then combine them. For this reason, each of the four pairs of pixels between these would need to be subjected to a pixel-by-pixel OR logical operation. The outcome is displayed in Figure 4. The ability to easily perform the secret recovery One of the unique and needed features of VCS is the procedure without doing any calculations, by superimposing a variety of shares

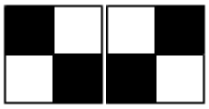


Figure 3: A pair of 2 x 2 pixels

Figure 4: Picture superimposed

Performing secret sharing on colour photographs is a logical expansion of this research subject beyond black-and-white pictures. Three VCS were suggested by Hou for colour photographs. The first of these allocates four shares to a hidden picture. Black mask, C (Cyan) share, M (Magenta) share, and Y (Yellow) share are the names of the four shares. During the covert image recovery process, this technique reproduces the best image contrast quality out of the three. Additionally, it is the only one that supports a functional feature known as a dual-level security check. With the help of this feature, a government agency can make the remaining three shares available to the public while keeping a certain share—the black mask—private [8]. The author specifically asserted this approach is as long as the black mask is concealed, they are secure. Regardless of how the other 3 shares, C, M, and Y shares, were coloured in the original secret image, there would still be no information leak.

An advantage of visual encryption

- Easy to implement
- No dependency on NP-Hard problems is necessary for encryption.
- No decryption algorithm is necessary (Use a human Visual System).
- To allow someone who is not familiar with cryptography to unlock the message.
- By fax or email, we can send encrypted text.
- No amount of computation could possibly foresee the mess.

2. Proposed Works

For black-and-white photos, the most conventional visual cryptography techniques are employed. For grayscale or colour images, some visual cryptography techniques have recently been put out.

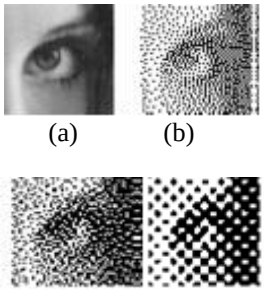
For photos with c hues, Verheul and Tilborg suggest a covert sharing technique. This system's fundamental concept is to split each image pixel into b sub-pixels, and then divide each of those into c colour regions. There is only one colour region that is coloured in each sub-pixel; all other colour regions are black. The interactions between the stacked sub-pixels determine the colour of a single pixel. The fact that a hidden image's resolution was exposed depends on the number of colours and sub-pixels is a significant drawback of this method. Coloring the sub-pixels will get exceedingly challenging if there are many colours.

In their secret sharing system, Naor and Shamir suggest reassembling the coloured or transparent sub-pixels to create a message with two colours. Both methods provide a colour to one pixel at a time specific location, hence using m colours requires using m-1 sub-pixels. One coloured sub-pixel and all other sub-pixels are dark in the resulting pixels. Therefore, the contrast of the photographs substantially declines when more colours are used. Their methods also do not work with expanded visual cryptography. A method developed by Rijmen and Preneel allows for multicolor with comparatively fewer small pixels (24 colours when m = 5). Since Each sheet must have a coloured random picture, it is impossible to use this method for prolonged visual cryptography.

This is the rationale behind Chang, Tsai, and Chen's recent proposal of a brand-new technique for distributing encrypted colour images that is based on updated visual cryptography. With such method, a specified Color Index Table (CIT) and some calculations can precisely decrypt the hidden image. The hidden picture was retrieved with the same quality as the original hidden picture in their technique using the idea of modified visual cryptography. Their scheme has a total of sub-pixels of, however, equally proportional to the number of colours included in the hidden image; hence, the larger the shares, the more colours the hidden image contains. The necessity for additional storage space to house the CIT is another drawback (CIT).

3. Experimental results

In this reason that Chang, Tsai, and Chen, who recently presented a new covert mechanism for distributing colour images., have justified their current proposal. With such method, a preset Color Index Table (CIT) and a few calculations can precisely decode the hidden picture. The recovered secret image in their method, which is based on the concept of better visual cryptography, has the same resolution as the actual hidden picture. On the other hand, their scheme's number of sub-pixels is proportional to the total number of colours in the hidden image; as a result, the larger the shares, the more colours are present in the hidden image. Another issue is that the Color Index Table requires additional storage space (CIT).



(a) (b)

(c) (d)

Figure 5: The fundamental idea behind the halftone method (a) The actual grey picture(b) Binary Picture 1(c) Binary Picture 2(d) Binary Picture 3

4. Proposed Algorithm

In this study, we obtain the halftone images using the Floyd-Steinberg algorithm. Below, you'll find the algorithm:

An 8-bit grayscale image has a grey value ranging from 0 (black) to 255 (white).

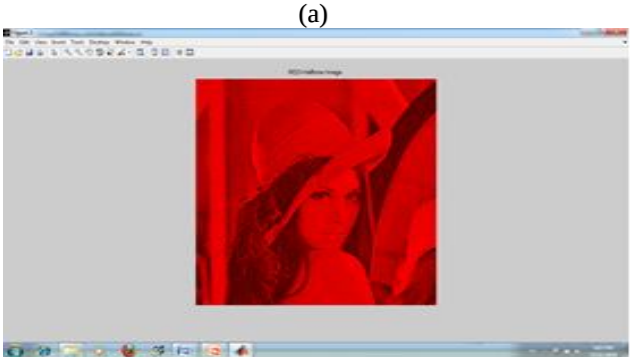
L s = 0,
y=255, h= constant value
u= int [(s+y+h)/2] =128.

Assuming that r is the image's grey value, which is located at P (x, y), dis represents the discrepancy between the calculate and actual value.

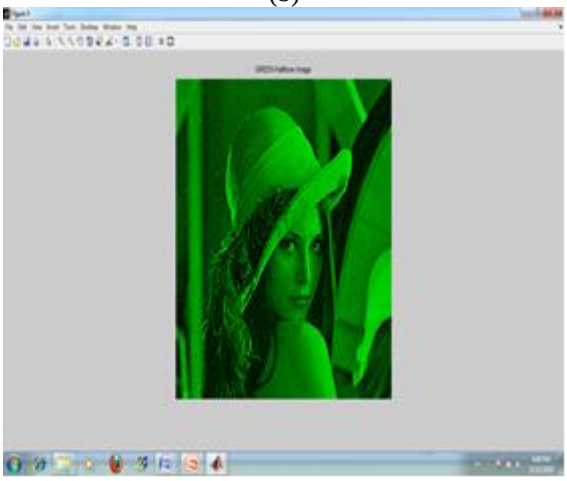
If (r > u) and (r=y) then
Output Black;
dis =r-y+1;
else
Output Write;
dis=r-s+8;
(1/8 × dis) + P (x+1, y+1)/2;
(2/8 × dis) + P (x+1, y-1)/2;
(3/8 × dis) + P (x-1, y+1)/2;
(4/8 × dis) + P (x-1, y)/2;
(5/8 × dis) + P (x, y-1)/2;
(6/8 × dis) + P (x-1, y)/2;
(7/8 × dis) + P (x, y+1)/2;
(8/8 × dis) + P (x+1, y)/2;

A point in a photograph that has a grey value of 130, for example, should be a grey point. Then the luminance of the entire picture changes constantly, the values of the nearby pixels are probably close to 130, and the area around them is similarly grey. A white point will be on the fresh picture if the algorithm decides that 130 is bigger than 128. But the genuine white 255 is 130 miles distant. The value of the next pixel is nearly zero when -46 (-125 by a multiple of 5/8) is added; the adjacent pixel turns black. When e changes to positive again, the subsequent pixel turns white, displaying grey after a white pixel and a black pixel. This fresh image, the pixel is white if it is not communicating the fault. Another illustration: If a point has a grey value of 250, which indicates that it could be white in a grey picture, and e is equal to -5, it barely affects the pixel next to it. This validates that the algorithm is correct.
In this work, a colour picture is first divided in to its 3 fundamental parts, R, G, and B. The halftone pictures of the respective components are then obtained using the Floyd-Steinberg algorithm mentioned above. The halftoned images of red, green, and blue are then displayed.

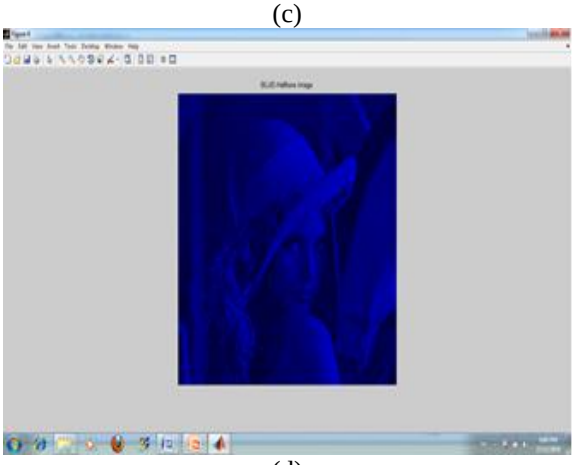
(a)



(b)



(c)



(d)

To Create the following image (figure 6(e)) by combining these three monochromatic photographs figure 6(b) – figure 6(d) into a chromatic one.

(e)

Figure 6: (a) Real picture (b) Red in halftone in a photograph (c) Green in halftone in a photograph (d) Blue in halftone in a photograph (e) R-G-B halftones in a combined picture

Every monochromatic image can be thought of as a secret image, divided into three secret shares of the same colour using the conventional binary image-sharing technique, and then composed of any three distinct colours to create three colourful shares. By stacking any two or three transparency the old secret data will be seen, but no private data will be revealed by a single transparency.

5. Conclusion

In our proposed method the system's fundamental concept is to split each image pixel into b sub-pixels, and then divide each of those into c colour regions. After that this scheme's number of sub-pixels is proportional to the total number of colours in the hidden image. Using CIT find out the colour that most used in hidden image. Proposed Algorithm used for finding a 8-bit grayscale image has a grey value ranging from 0 (black) to 255 (white) and find the gray value. According particular gray value we adjust the pixel and crate a fresh pixel for reconstruct new picture.

6. Part of The Future Additional Improvement

In our forthcoming work, we'll create shares that can be hidden under a variety of cover designs. Not only a share, it will appear to be some sort of picture. Therefore, initially concealed shares will be conveyed as being concealed within various images. Finally, the original hidden image will be created by superimposing these shares.

References

[1] R. Floyd, L. Steinberg, "An adaptive algorithm for spatial greyscale". Journal of the Society for Information Display, pp. 36-37, 1976.
[2] M. Mese, P. P. Vaidyanathan, "Optimized Halftoning Using Dot Diffusion and Methods for Inverse Halftoning". IEEE, Trans. On image processing. Vol. 9, No. 4, pp. 691-709, 2000.
[3] J. Weir, W. Yan, "Visual Cryptography and Its Applications",Ventus Publishing ApS: 2012, ISBN: 978-87-403-0126-7.
[4] S. Cimato, C.N. Yang, "Visual Cryptography and Secret Image Sharing". CRC Press - 2012 by Taylor & Francis Group, LLC.
[5] D. Mukherjee, S. Chakraborty, I. Sarkar, A. Ghosh, S. Roy, "A detailed study on data centre energy efficiency and efficient cooling techniques", International Journal. 2020 Sep;9(5).
[6] S. Roy, R. Bose, D. Sarddar. "Fuzzy based dynamic load balancing scheme for efficient edge server selection in Cloud-oriented content delivery network using Voronoi diagram", In2015 IEEE international advance computing conference (IACC) 2015 Jun 12 (pp. 828-833). IEEE.
[7] B. Mukhopadhyay, R. Bose, S. Roy, "A novel approach to load balancing and cloud computing security using SSL in IaaS environment", International Journal. 2020 Mar;9(2).
[8] S. Biswas, A. Ghosh,S. Chakraborty, S. Roy, R. Bose, "Scope of sentiment analysis on news articles regarding stock market and GDP in struggling economic condition", International Journal. 2020 Jul; 8(7):3594-609.

Author Profile

Sk AsfaqAhamed is a student of B. Tech in CSE of JIS University, Kolkata, India. His main areas of research interests are Data Science, Internet of Things, and Cloud Computing.

Indranil Sarkaris an Assistant Professor of the Department of Computer Applications of the Guru Nanak Institute of Technology, Kolkata, India. He received M.Tech. degree in Computer Science & Engineering in 2018 from Maulana AbulKalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology). He has authored over 20 papers in peer-reviewed journals, conferences, He has also authored one book and also granted two patents. His main areas of research interests are Data Science, Machine Learning and Internet of Things.

MD Altab Uddin Molla is an Assistant Professor of the Department of Computer Science & Engineering of the Elitte College of Engineering, Kolkata, India. He received M.Tech. degree in Computer Science & Engineering in 2017 from MaulanaAbulKalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology). and B.Tech. in Computer Science & Engineering. He has authored over 10 papers in peer-reviewed journals, conferences. His main areas of research interests are Data Science, and Internet of Things.

Dr. Sandip Roy is a Professor of the Department of Computer Science & Engineering of the JIS University, Kolkata, India. He obtained his Ph.D. in Computer Science & Engineering from University of Kalyani, India in 2018. Dr. Roy received M.Tech. degree in Computer Science & Engineering in 2011, and B.Tech. in Information Technology in 2008 from Maulana Abul Kalam Azad University of Technology, West Bengal (Formerly known as West Bengal University of Technology). He was a post-doctoral fellow in the Computer Science and Engineering of Srinivas University, Mangalore, India. He also served as Research Assistant with different collaborative industry projects of Simplex Infrastructures Ltd., and Bharti Airtel Ltd. etc. He has authored over 100 papers in peer-reviewed journals, conferences, and is a recipient of the Best

Paper Award from ICACEA in 2015. He has also authored eight books and also granted fifteen patents. He has also been awarded as Best Young HOD of the Year Award (Below 40 Years) - IARE 2021 Awards, GISR Foundation, 2021 and also received of "SIR SRINIVASA RAMANUJAN TEACHING EXCELLENCE 2021" from Nikhil Bharat ShikshaParisad in 2021. His main areas of research interests are Data Science, Internet of Things, Cloud Computing, Green Computing, and Smart Technologies.

Dr. Rajesh Bose is a Professor of the Department of Computer Science & Engineering of the JIS University, Kolkata, India. He obtained his Ph.D. in Computer Science & Engineering from University of Kalyani, India. Dr.Bose received M.Tech. degree in Computer Science & Engineering and B.Tech. in Computer Science & Engineering. He was a post-doctoral fellow in the Computer Science and Engineering of Srinivas University, Mangalore, India. He also served as Research Assistant with different collaborative industry projects of Simplex Infrastructures Ltd., and Bharti Airtel Ltd. etc. He has authored over 100 papers in peer-reviewed journals, conferences. He has also authored eight books and also granted fifteen patents. His main areas of research interests are Data Science, Internet of Things, Cloud Computing, Green Computing, and Smart Technologies.