Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6040902, 12 pages
https://doi.org/10.1155/2022/6040902

Research Article

CMY Color Spaced-Based Visual Cryptography Scheme for Secret Sharing of Data

Anli Sherine,[1] **Geno Peter**,[2] **Albert Alexander Stonier**,[3] **K. Praghash**,[4] **and Vivekananda Ganji**[5]

[1]*School of Computing and Creative Media, University of Technology Sarawak, Malaysia*
[2]*CRISD, School of Engineering and Technology, University of Technology Sarawak, Malaysia*
[3]*Department of Electrical and Electronics Engineering, Kongu Engineering College, India*
[4]*Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, India*
[5]*Department of Electrical and Computer Engineering, Debre Tabor University, Ethiopia*

Correspondence should be addressed to Vivekananda Ganji; drvivek@bhu.edu.et

Received 20 January 2022; Accepted 21 February 2022; Published 9 March 2022

Academic Editor: Deepak Kumar Jain

Visual cryptography technique allows visual information to be encrypted in such a way that the decrypted information appears as a visual image. Visual cryptography allows digital images to be separate into few shares called transparent shares. For security reasons, it ensures that hackers cannot find any clues about the secret image from a single cover image. The proposed technique uses CMY (cyan, magenta, yellow) color space to enhance visual cryptography, and mean visual cryptography can be used on color images. The other techniques used were color decomposition and error diffusion. Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. The image will be encrypted by four shares which is cyan, magenta, yellow, and mask. Mask will be using random function to random generate half black and half white pixel in 2×2 block. Stack all the shares for reviewing the secret image. After that, do the image preprocessing of the image and use OCR (optical character recognition) to recognize the message.

1. Introduction

With the development of science and technology, people's lives have changed greatly. In this age of information, the internet has become an indispensable channel. It is spread all over the world, and it is getting closer to human life. Everyone knows that internet is a modern high-tech product that contains a lot of knowledge. There has a lot of learning materials on the internet for people to learn, and online searching information is faster and convenient. More than that, news, weather forecasts, life information, and people can all see through the internet. In a society where information flows at high speed, the secret management has always been a compelling issue in our life. Now is the era of internet, and the internet is always used by individuals to communication. People are passing and accessing information through the internet, but this can easily lead to information leakage. When important things and information are reliably protected, possible abuse or misfortune can be avoided. Cryptography is the science of information security. The main objective of cryptography is doing the information hiding. Secret sharing is referring to any secret method of allocation among a group of participants, and each participant is assigned secret share in visual cryptography. Security key management is the biggest motivation for secret sharing. In certain cases, only one key provides access to many important files. All important files will become inaccessible when the key is lost. The secret can only be reconstructed when the shares are merged together. A single share itself has no use. When conditions are fulfilled, then the secret will be open. Now, visual cryptography can be used on the grey images and RGB/CMY images. RGB/CMY is the color image. RGB is the color space for digital images, and it is red, green and blue. In RGB, the light source in the device

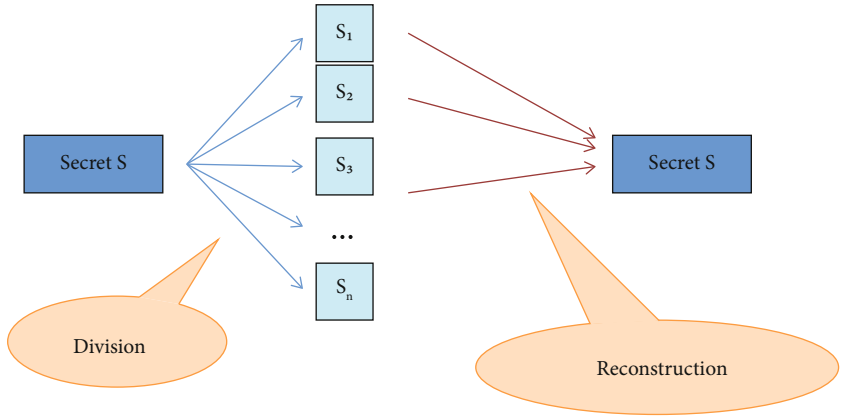


Figure 1: Example of secret sharing.

creates any color by mixing red, green, blue and changing its intensity. This is like an additive blending, and all colors start with black, then red, green and blue light which superimposed on each other to make them brighter and form the perfect pigment. When red, green, and blue light which are mixed together with the same intensity, it will produce pure white. The CMY color model can be called like a subtractive color model, and it consists of cyan, magenta and yellow. Verheul and Van Tilborg are the first proposed the visual cryptography scheme for color images in the second half of 1997. One important thing is only the person with all n shares can do the decryption with that image, and $n-1$ share does not display information about the original image where the image is separated into n share. In Figure 1 below, the secret image will divide to few images, and S means the several part of the image.

2. Related Work

In the era of technological progress, the internet has been always used by the people for the transmission and acquisition of communication and information. In order to protect our data from illegal processing and to ensure the security and security of confidential information, everyone uses symmetric or asymmetric encryption techniques. However, the encryption process requires more execution cost. Therefore, there are many suggestions and recommendations on the methods of secret sharing schemes. By dividing the secret into multiple copies, secret image distribution is an excellent skill and talent for protecting important image's information. The rationale behind this scenario is to transform the color image to a number of unreadable format type shares. So, people only can see the information in the image by combining some mathematical calculations and some mathematical calculations. Security, reconstruction accuracy, computational complexity, and storage requirement are the four conditions for determining a secret sharing scheme. There has a problem associated with the image security in most of the previous scheme. It was because people cannot see the hidden message when all share images are not stack together. The second problem is the quality of the reconstruction image. This means that the reconstructed image loses some of the information, and the resulting image is not same with the original image. Data loss occurs because the image is affected by pixel expansion issues. Now, people will achieve the CMY color space on the color image using a visual cryptography-based $((n-1), n)$ secret sharing scheme and do the comparison. It solves the security, pixel expansion and accuracy issues. Other than this, the cyan, magenta, yellow, and black (CMY) also use by the printer.

2.1. Visual Cryptography. There are few traditional symmetric and asymmetric encryption methods, for example, Advanced Encryption Standard, RSA, and Data Encryption Standard, and it requires complex cryptography and need more time to complete the process [1]. Therefore, there is an urgent need for a lightweight method for encrypting secrets. Moreover, in some situation, if only one person keeps the secret data file without additional copies, it is dangerous because the secret data file may be accidentally lost, intentionally modified, or destroyed by a malicious attacker [1]. For these cases, in order to ensure the security of the secret, a group of people need to share a secret data file. So, Shamir proposed the concept of encryption in 1979 to solve this kind of problem, that is, (k, n) threshold secret sharing [1]. K means that the secret K is divided into n mapped shares; N means the number of participants. This method is intended to transfer confidential data files to n share and distribute n participant. This method means collected each k or more shares can restore the confidential image, but every $k-1$ is unable to obtain information about the confidential image. $K-1$ is mean less than k share. According to Naor and Shamir, [2] proposed the (k, k) threshold visual secret sharing, which enabled the low computational encryption process to be realized in year 1994. Since then, in year 1995, the idea or concept of visual cryptography will be proposed by this two people. Visual cryptography is a paradigm that can decrypt image. The most striking feature of this method is that it no need do calculations to reveal the confidential image. It overcomes the shortcomings of the complex calculations required by traditional cryptography. Visual cryptography uses the human visual system to view confidential messages from overlap in the share. The secret message can be picture or text. It is

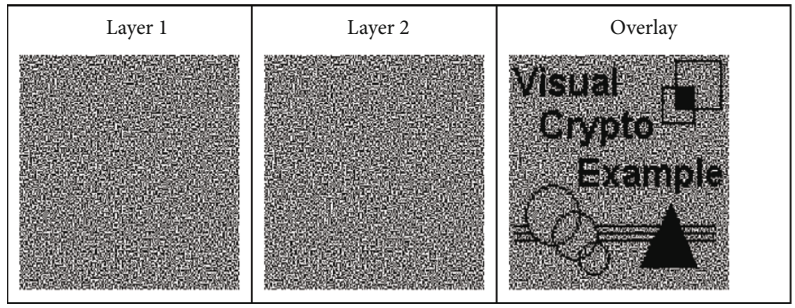


Figure 2: Visual secret sharing scheme (image retrieved from [3]).

simple and completely secure method that allow for secret sharing, which they call visual cryptography scheme (VCS). About the secret sharing concept, the encryption process encrypts confidential images into shares, and these shares are noise-like security image and print on transparencies. Every transparency that share will look like a random binary pattern. This share can send out in public communication channel. Then, using human visual system attributes to press the identification of confidential messages from shares overlap, without the need for additional calculations and any cryptography knowledge to decrypt secret images. The main example of visual cryptography implements an encryption protocol called secret sharing. The secret image is splitting into n shares, so just the administrator who owns all n shares can do decryption with that image, and any $n-1$ shares will not show any message regarding the confidential image. Considering the low computational complexity and simple process, this technique is well suited for encrypting shared secret images and using the human vision to decrypt secret. In addition, visual cryptography does not require the construction of a secret key but has a fast and convenient decryption technology, which can improve efficiency. So, there is no longer a need to worry about the loss of keys or the cruel method of trying key values in visual cryptography. Just a group of people stacked together owned shares, and the secret image can be displayed safely and effectively in a timely manner. As shown in Figure 2, under the (k, n) visual secret sharing mechanism, in a total of n shared images, it must be greater than or equal to k shared image overlay to interpret the confidential image, as long as the number of overlapping shared images is less than k, and it cannot be decrypted. However, it only suitable for binary images in black and white, and the resulting shared images are meaningless. In addition, since the rule for sharing images is to represent the black or white of one original pixel in 4 pixels, so the size of shared and the restored image must be expanded to 4 times the primitive image.

The shared images produced by the Naor and Shamir methods are garbled and have no meaning. However, if that sharing image can be share into a meaningful image, it will not cause suspicion from interested person, more camouflage function, and beautiful effect. In 2001, Hwang and Chang proposed an improved (k, n) visual secret sharing scheme, which can generate two meaningful shared images, as shown in Figure 2, which uses a 3×3 pixel expansion instead of a 2×2 pixel expansion method, and it makes the black and white definition more flexible, resulting in meaningful sharing of images. In Figure 2, layer 1 and layer 2 show different message, and the secret message will come out after overlap this two layer. In 2001, Hwang and Chang proposed an improved (k, n) visual secret sharing scheme, which can generate two meaningful shared images; as shown in Figure 3, which uses a 3×3 pixel expansion instead of a 2×2 pixel expansion method, it makes the black and white definition more flexible, resulting in meaningful sharing of images. In Figure 3, layer 1 and layer 2 show different messages, and the secret message will come out after overlap this two layer. Hou converts the grayscale image to a halftone image and exploit the binary visual cryptography scheme to produce the grayscale fraction. Although the confidential image is a grayscale image, the sharing is still made up of a random binary pattern that carries visual information, which may lead to doubts about confidential encryption. The idea of color mixture of two-out-of-two visual cryptography scheme is presented by Rijmen.

A third mixed color will come out when two transparent films of different colors are stacked. Halftone methods and color decomposition are sharing by Hou. In 2003, Hou breaks down the confidential color image into three halftone images (cyan, yellow, magenta) which is CMY color space [5] as shown in Figure 4. Then, Hou designed three colored (2) visual cryptography schemes by using some of the existing binary visual cryptography schemes, followed by color mixing of the subtractive model. The principle is to first transform into three halftone shared images corresponding to Y, M, and C colors, according to the visual cryptography rule, and the image is decomposing into six shared images Y_1, M_1, and C_1 and Y_2, M_2, and C_2. Then, Y_1, M_1, and C_1 are combined to form a first shared image, Y_2, M_2, and C_2 are formed the second shared image, the decryption process does not need to be calculated by a computer, and only two shared images are overlapped for decrypted.

3. Proposed Methodology

The proposed technique determines that the secret sharing scheme with CMY color space is visual cryptography. Visual cryptography is an algorithm that is used to encrypt and decrypt the image. Visual Cryptogrpahy involves image processing, dividing the original image to few halftone images for encryption and later combining all the images for

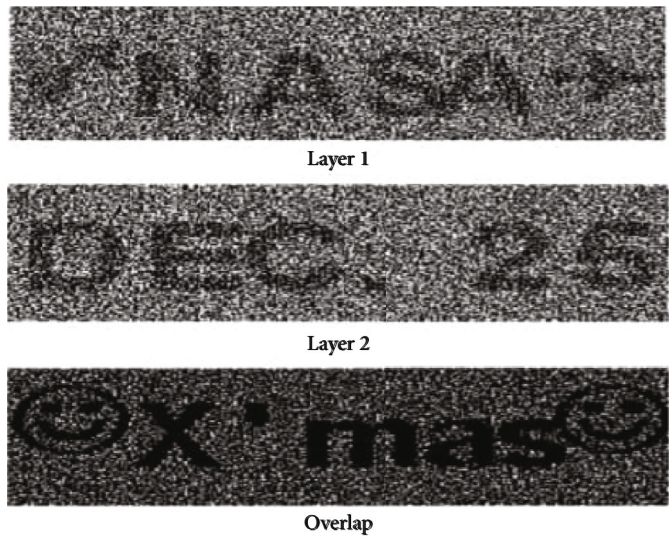


Figure 3: Meaningful camouflage image (image retrieved from the [4]).

Figure 4: Visual cryptography of color space (image retrieved from [5]).

decryption. A method for image processing is performed on the image in order to obtain increase image certain operation or to pick up some beneficial information. Import image for doing analyzing and processing of the image. The output can change the image or image analysis-based reports. Convert an image from RGB to the CMY color space through the image processing. For the encryption, separate the original image to halftone image using color decomposition. Then, use the error diffusion to encrypt the halftone image with a pair of pixel. This kind of component image is like a transparent, and no one can see the image behind the scheme. For the decryption, combine all of the sharing images to reveal the confidential image. In additional to this, image histogram was also created. It was used to show the difference between the original image and decryption image. First, user needs to load a new image, and the image type must be JPG or PNG [6]. Then, image will direct convert to Qt format. Second, choose the scheme which is RGB or CMY to generate the shares. If the user does not select the scheme, system will pop up an error message and continue at the same step. Third, generate the shares according to the user's choice. In this step, system will split the red, green, and blue components of the image. Then, convert these three colors to cyan, magenta, and yellow when the user chooses the CMY scheme. The conversion is given by the formulae cyan = 255 minus red, magenta = 255 minus green, and yellow = 255 minus blue. After that, system will convert CMY to halftone with the error diffusion. Using the middle intensity which is 128 to do the calculation until each pixel becomes 255 or 0, besides, generate a mask with the random half white and half black pixel. Fourth, combine all of the shares and masks to display the secret image. In this step, user needs to click the checkbox to combine all the shares [7]. Then, system will do the calculation. Set the intensity of the shares that becomes 128 when the pixel value of mask is 0, otherwise, minus by 255. Lastly, click the save button to create a file and save the output of the image and the shares with the PNG image type. The flowchart of the proposed system is shown in Figure 5.

3.1. System Environment. The tools used in this research are Qt Creator. Qt is a cross platform applications and free open source widget toolkit for establish graphical user interfaces. It can run on a variety of software and hardware platforms. In addition, Qt provides stability to the user. The library uses in this research is OpenCV. It is a programming function

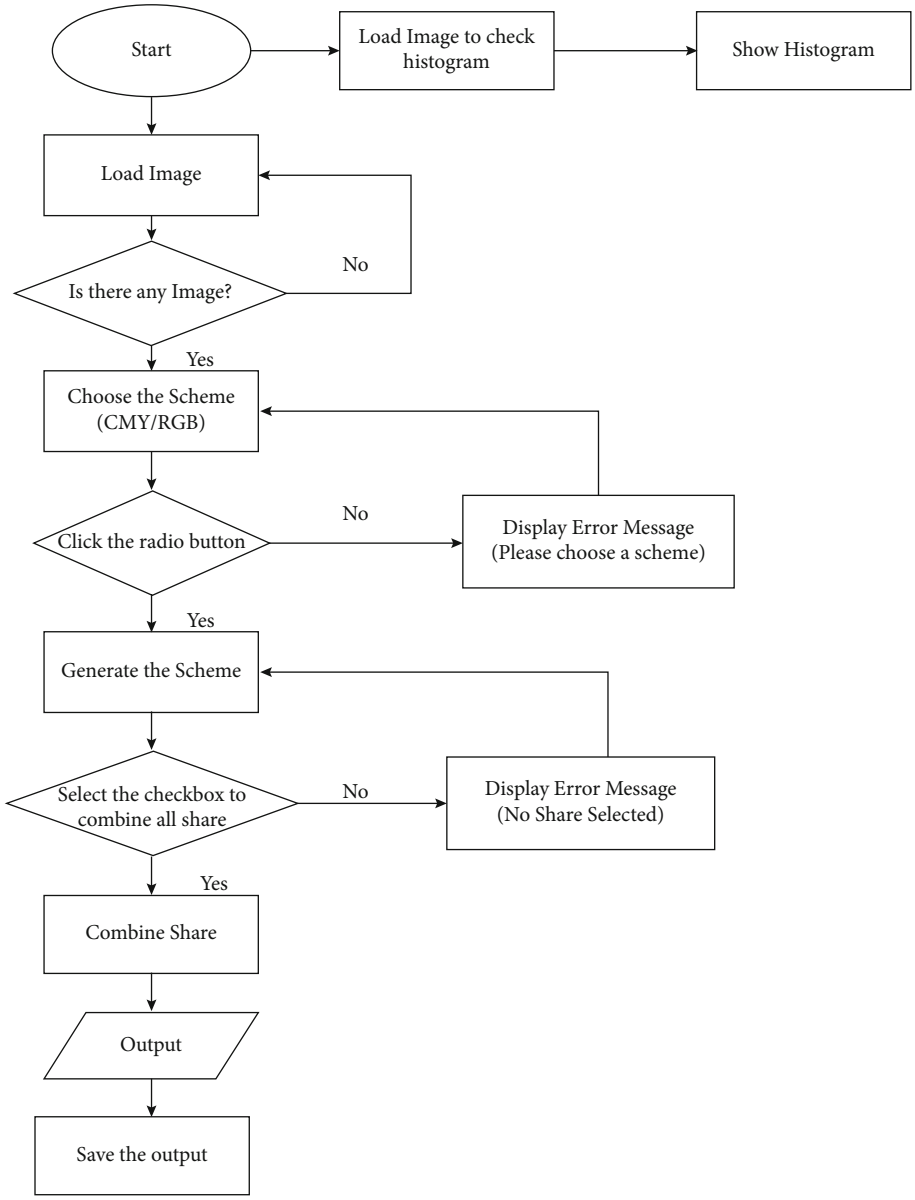


Figure 5: Flow chart of the proposed system.

Table 1: Results of encryption and decryption (CMY).

Type	Sample images	Clear	Unclear	Accuracy
512 × 512 JPG	30	28	2	93.3%
512 × 512 PNG	30	27	3	90%
640 × 480 JPG	30	24	6	80%
640 × 480 PNG	30	22	8	73.3%
1920 × 1080 JPG	30	30	0	100%
1920 × 1080 PNG	30	30	0	100%
4000 × 3000 JPG	10	10	0	100%
4000 × 3000 PNG	10	10	0	100%
Average				90.5%

library mainly for real-time computer vision. The library has its own image type, Mat, which is a matric containing all pixel values of the image. This simplified the process of checking and manipulating pixel values significantly.

3.2. Image Type. The image is a description of the visual perception of artifacts. For example, it is a picture made using a camera or other two-dimensional picture (screen display or photograph). Images is the magnitude of the distribution of one or more colors [8]. It can capture by optical equipment, for instance, microscopes, telescopes, lenses, mirrors and camera. There are many kinds of images use in the visual cryptography such as grayscales images, binary image, and color images. But in this research, the color image will be chosen to do the visual cryptography. It was because the CMY components will separate from a color image. The image file format will be JPG and PNG. They are the most

Table 2: Results of encryption and decryption (RGB).

Type	Sample images	Clear	Unclear	Accuracy
512 × 512 JPG	30	0	30	0%
512 × 512 PNG	30	0	30	0%
640 × 480 JPG	30	0	30	0%
640 × 480 PNG	30	0	30	0%
1920 × 1080 JPG	30	0	30	0%
1920 × 1080 PNG	30	0	30	0%
4000 × 3000 JPG	10	0	30	0%
4000 × 3000 PNG	10	0	30	0%
Average				0%

popular file format that can easily get from the online resource. The most editing software can open the JPG and PNG files.

3.3. Image Processing. In the image processing, the imported image will convert from an RGB to CMY color space. Afterward, do the color decomposition for the import image before convert it to the halftone image. The cyan, magenta, and yellow colors will separate from the image for each pixel through the color decomposition. The following relationships of CMY and RGB: $C = 255 - R$, $M = 255 - G$, and $Y = 255 - B$. Thus, in the (C, M, Y) representation, (0, 0, 0) represents full white, and (255, 255, 255) represents full black.

3.4. Error Diffusion. Error diffusion is a kind of halftone in which quantized residuals are distributed to neighboring pixels that have not been processed. The main purpose is converting multilevel images to binary images; although, it has other application [9]. It is different with other half toning methods, and it is classified as a regional operation because the operations performed by the algorithm at one location affect the operations that occur at other locations. Error diffusion with edge enhanced image tendency. Compared to other halftone techniques, this can make the image's text more readability. This method captures monochrome or color images and decreases the amount of quantization levels. The general application of error diffusion related reducing the number of quantized states to only two per channel which is 255 or 0 [10]. There are many types of error diffusion, but only one-dimension error diffusion is used. The simplest form of this algorithm is to scan one pixel and one row with an image at a time, compared the current pixel with the half gray value. If it is higher than this value, white pixels will be generated in the generated image. If the pixel is less than half the brightness, black pixels are generated. The resulting pixels are completely bright or completely black; so, there are errors in the image. Then, add the error to the next pixel in the image and repeat the process. For example, the greyscale value is 100 of a pixel. This value is closer 0 than 255; so, it will automatically become 0, and 100 (the error) will be add into the next value.

3.5. Encryption and Decryption. Encryption is a way to hide the information into the true meaning of the information through the secret code method. An encryption data is also called cipher text, and it looks like a plaintext. The encrypted algorithms are a formulas use to encode the information. Then, the visual image will be displayed by the decrypted information [11]. The process of converting encrypt data to its original format is called decryption. Choose all of the shared images for doing the combination. Only by overlaying all the images can more clearly restored the secret image. The algorithms use in encryption and decryption is visual cryptography [12]. Before starting to encrypt and encrypt an image, choose an image and import the image from the file directory to the system. After that, image processing is done to convert the RGB to CMY color space. After converting to CMY color space, the visual cryptography process is as follows:

(i) Divide the image to three color component images (C, M, and Y)

(ii) Error diffusion will be use to generate the halftone image. All the pixel of the halftone image will be expanded to 2 × 2 block. Therefore, each block of the shared image contains two transparent (white) pixels and two-colored pixels

(iii) Create a black and white share, known as a mask, which is double the size of the secret image in each direction. The block of pixels will randomly assign half black and half white in this mask

(iv) Selecting the mask for check the pixel value, if cyan component is revealing, fill the positions corresponding to the position of the white pixels in the mask with a cyan pixel and the color to the opposite way

(v) According with (IV), do the same thing to check the magenta and yellow pixel value

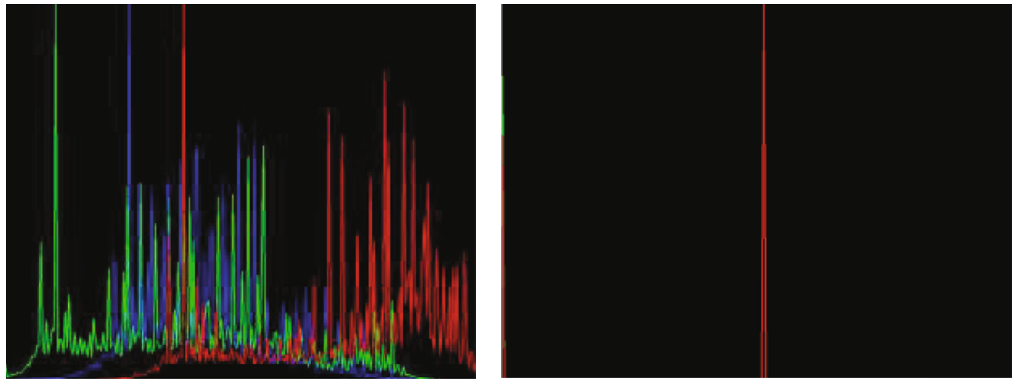
(vi) Repeating the steps (IV and V) until all pixel in the image is decomposed, then get the four-sharing image which is cyan, magenta, yellow, and black

(vii) Lastly, using the four-sharing image and stack together, the value of pixel in mask is 0 will become 128; otherwise, it will be minus by 255, and the confidential image will be decrypted by human visual system

3.6. Histogram. The image histogram is a histogram that can be used as graphical representation of the distribution of tones. The amount of contrast will describe by a histogram. It will calculate the brightness and darkness in a scene. In the program, it loads an image to do testing. Using Open CV function "Split", the image is divided into R, G, and B planes, hence three different colour lines will be shown in the histogram image. Third, using OpenCV function "calcHist" to calculate each R, G, and B planes of the histogram, the important things in here are BINS, DIMS, and RANGE.

(a) (b)

Figure 6: (a) Result of RGB image. (b) Result of CMY image.



(a) (b)

Figure 7: (a) Original image histogram. (b) CMY image histogram.

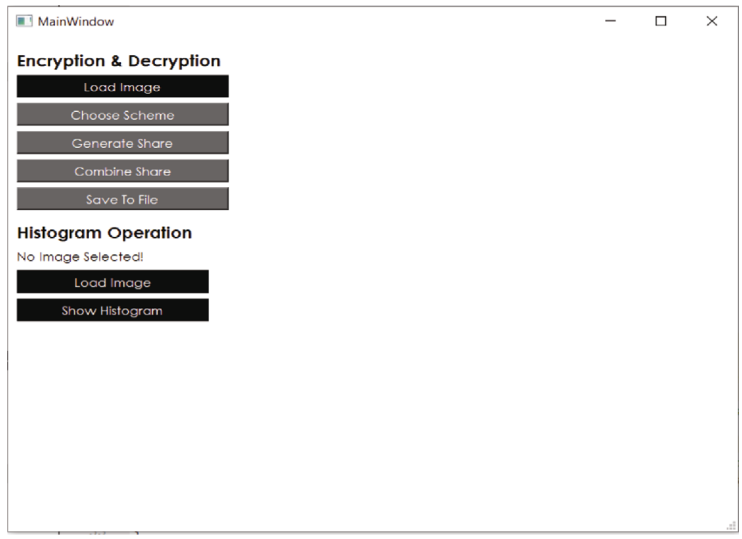
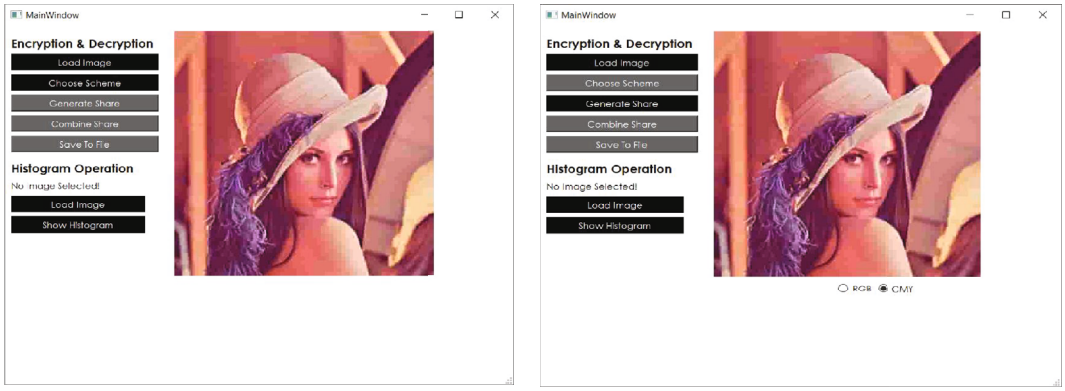


Figure 8: Main page.

BINS means the number of pixels. Normally, it will be 256. DIMS means the number of parameters for data collect [13]. In the program, DIMS value is always 1 as it refers to the intensity value of the data collected. RANGE means the intensity value. Normally, it will be [0, 256]. Lastly, plot the three line of histogram in a new window.



(a) (b)

Figure 9: (a) Process of loading image. (b) Process of choose scheme.

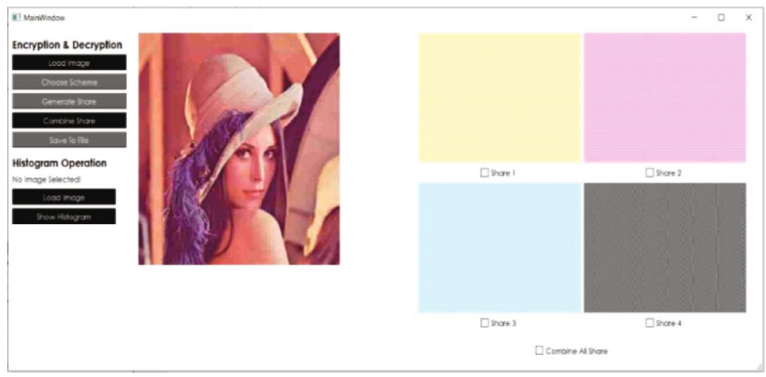


Figure 10: Process of generate share.

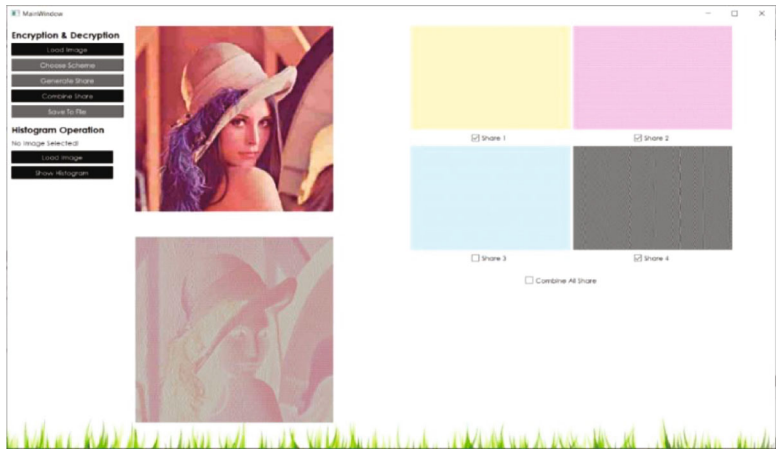


Figure 11: Incorrect result of decryption.

4. Results and Discussions

The system was implemented by using the proposed method which is error diffusion and visual cryptography algorithm. There are 200 sample images that are used for testing in this research. The secret image will divide by four halftone images which is cyan, magenta, yellow, and black. Code sharing images of four completely confusing, people cannot find out any clues to the confidential image from any single shared image. The result of average accuracy for both type of images is calculated and is shown in Tables 1 and 2 .There are two types of images used in this research which is JPG and PNG. The images will be divided into 4 different sizes. The size includes 512×512, 640×480, 1920×1080, and 4000×3000. There are 30 images of 512×512 size for both JPG and PNG, 30 images of 640×480 size for both JPG and PNG, 30 images of 1920×1080 size for both JPG and PNG, and 10 images of 4000×3000 size for both JPG and PNG. Actually, the landscape and portrait are not difficult to distinguish, but the clarity of the picture varies. The highest

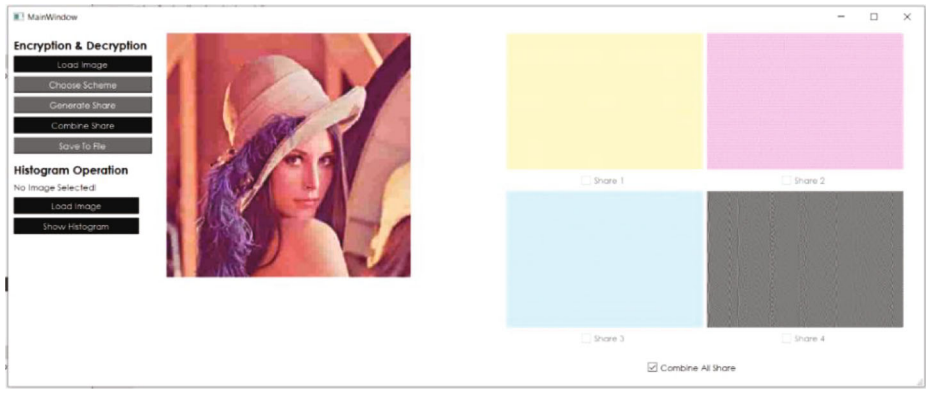
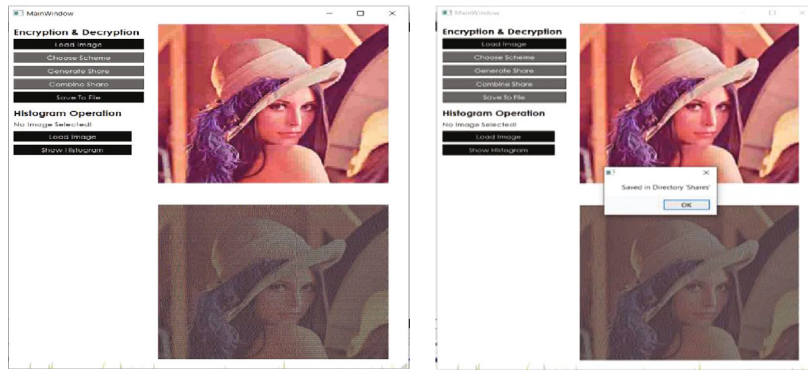
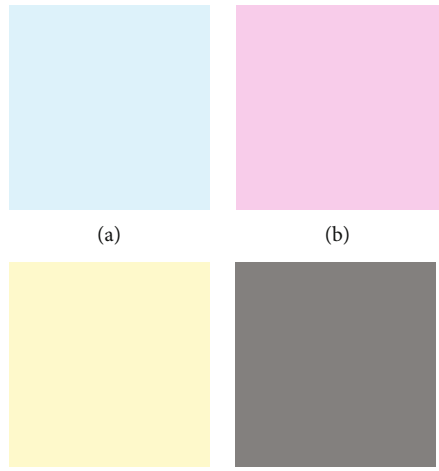


Figure 12: Checkbox for combine all share.



(a) (b)

Figure 13: (a) Correct result of decryption. (b) Save image to file.



(a) (b)

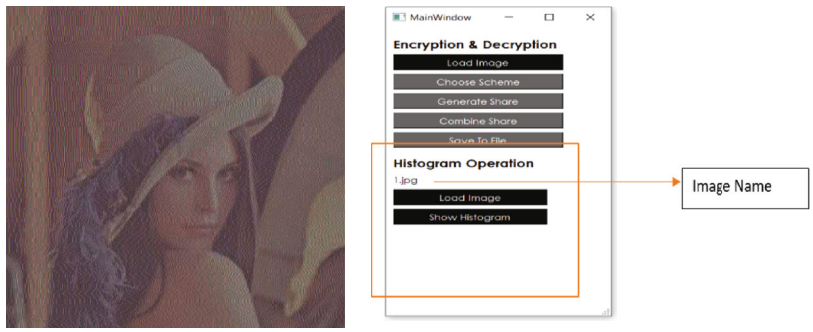
(c) (d)

Figure 14: (a) Cyan image. (b) Magenta image. (c) Yellow image. (d) Mask.

recognizable image size is 1920 × 1080 and 4000 × 3000. The smallest font is mostly unclear when the image size is 512 × 512 and 640 × 480. So, the conclusion is the image resolution will affect the clarity of image.

4.1. Differences between CMY and RGB Image. The image that was used to encrypt with the CMY will look better than RGB. The output of encryption with RGB was dark and not clear than CMY as shown in Figures 6(a) and 6(b). The output of encryption with CMY was bright and clear.

4.2. Differentiate the Histogram. In fact, visual cryptography with CMY color space in halftone image will loss the image's contrast. All of the final result about the histogram would



(a) (b)

Figure 15: (a) Output of secret image. (b) Histogram operation.

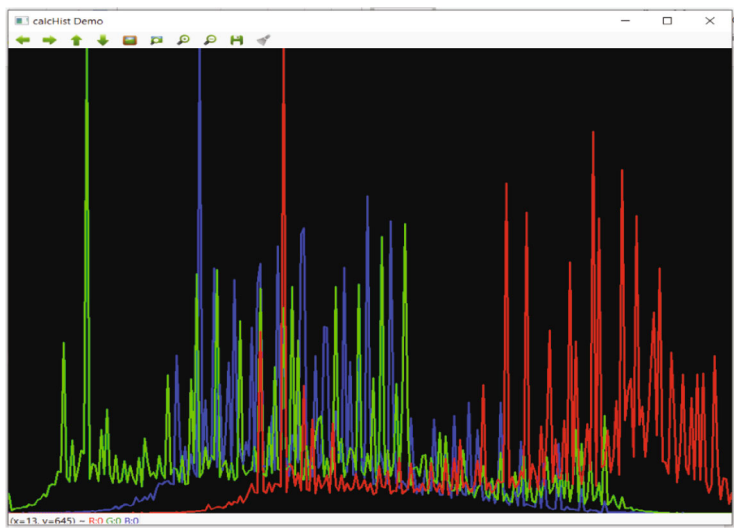


Figure 16: Image histogram.

look like same. The image histogram will look like low contrast after decryption. The image test by RGB is brightness, and the image test by CMY will be darkness. It is like an extreme as shown in Figures 7(a) and 7(b).

4.3. Proposed Technique Results. The system consists of two different parts which are encryption/decryption operation and histogram operation. User can choose either to encrypt/decrypt process or show image histogram process [14]. In Figure 8, there are five buttons shown in the encryption and decryption process. The button includes load image, chooses scheme, generates share, combines share, and saves to file, but only one button can be chosen when the user runs the system.

It was because user needs to load the image before to encrypt or decrypt. Another button is disabled the in encryption/decryption process. There are two buttons which is load image and show histogram in histogram process. There is a message "No Image Selected!" in histogram operation. Both buttons can be click. If user has no input any image and clicks the show histogram button, the error message will be pop up. Figure 9(a) shows the input image, and the choose scheme button is enabled [15]. Before user clicks the choose scheme button, user cannot click the generate share, combine share, and save to file button. Figure 9(b) shows the process of choose scheme. When user clicks the "choose scheme" button, there are two radio buttons that will come out which is RGB and CMY. User needs to choose one of the radio button before click the "Generate Share" button; otherwise, the error message will pop up. "Choose Scheme" button will become disabled, and "Generate Share" will become enabled.

Figure 10 shows the generate share process. When user clicks the "Generate Share" button, the button will become disabled, and the "Combine Share" button will become enabled [16]. The 4 different shares will show beside the input image. The 4 different shares will look like cyan, magenta, yellow, and black. There are four checkboxes under the share image. The four checkboxes are share 1, share 2, share 3, and share 4. It only shows when the image's width or high is less than 1000.

It uses to prove if user does not select to combine all share, and the output image will look like very big different with the original image. Another way of saying is it will not show the secret image. Then, it will stop in this step, and the save button will not be enable to click. Figure 11

below shows the incorrect result after decryption. It was because user only selects share 1, share 2, and share 4. The high-resolution image will bring the high accuracy. There are some limitations about the secret image, but it does not affect the protection brought by the encrypted picture and the accuracy brought by the decrypted picture. The highest recognizable image size is 1920×1080 and 4000×3000 in this research [17]. Relatively, the highest resolution image used needs more time to decrypt because the size of the image is larger. If compared to both color space for the encryption and decryption, CMY will be the successful example. The image using the CMY encryption is closer to the original picture.

Figure 12 above shows that the share 1, share 2, share 3, and share 4 will be disabled to click. It was because the user clicks the "Combine All Share" checkbox. This is a very convenient setting for the user.

Figure 13(a) above shows a correct output image after clicking the combine share button. So, the combine share will become disabled, and the button save to file will become enabled. Figure 13(b) above shows the message "Saved in Directory Shares" when user clicks the save to file button. Then, the save to file button will be disabled.

Figure 14(a) shows the cyan output that was saved in file directory. It was named share_1.png. Figure 14(b) shows the magenta output that was saved in file directory. It was named share_2.png. Figure 14(c) shows the yellow output that was saved in file directory. It was named share_3.png. Figure 14(d) shows the mask of the input image that was saved in file directory. It was named share_4.png.

Figure 15(a) shows the output that was saved in file directory. It will be named combined_share.png. Figure 15 (b) shows the histogram operation. The image name will show when the user loads the image.

Figure 16 shows the image histogram with the three lines which are red, green, and blue color. The histogram will open in a new window after the user clicks the button "Show Histogram."

5. Conclusion

Due to the widespread application of the Internet technology, data security has become a key factor today. In the human-based visual cryptography mechanism compared to the traditional cryptographic, it can realize a lower amount of computation and break away of complicated encrypt knowledge. This is one of the benefits of visual cryptography. Visual cryptography provides a secure way to transfer images. It also hides the information of the image. The visual encryption technology of CMY color space based on secret sharing leads people's attention because of its ability to maintain secrecy and hide the color information. The secrets cannot be judged after they are generated and distributed. The accuracy of CMY color space is better than RGB color space while the final image will be looked like darkness. The future work can be reducing the total time spend in the encryption and decryption of an image. In order to improve security, the digital watermarking and steganography can be used together with the visual cryptography, example, hiding some information in the image and encrypt with visual cryptography. In additional to this, the video file also can be divided into different frames to encrypt it and use the proposed algorithm to encrypt each frame.

Data Availability

The data will be available on request to the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C.-C. Chang, B. Li, and J.-S. Lee, "Secret sharing using visual cryptography," *Journal of Electronic Science and Technology*, vol. 8, no. 4, 2010.

[2] M. Naor and A. Shamir, "Visual cryptography. Improving the Contrast via the Cover Base," *Presented at Security in Communication Networks*, vol. 1189, pp. 197–202, 1997.

[3] D. Rijmenants, "Visual cryptography," 2004, http://users.telenet.be/d.rijmenants/index.htm.

[4] W.-L. Tai and Z.-J. Liao, *Color secret hiding based on visual cryptography*, vol. 22, no. 2, 2016Department of Information Communications, Chinese Culture University, 2016.

[5] Y.-C. Hou, *Visual cryptography for color images*, vol. 36, no. 2003, 2002, Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC, 2002.

[6] C. C. Chang, C. S. Tsai, and T. S. Chen, "A technique for sharing a secret color image," in *Proceedings of the Ninth National Conference on Information Security*, pp. LXIII–LXXII, Taichung, 1999.

[7] DataGenetics, "Visual cryptography," 2009, http://www.Datagenetics.

[8] A. G. Shirodkar, "Review of visual cryptography," *International Research Journal of Innovation Engineering*, vol. 1, no. 3, 2015.

[9] A. V. Dahata, "Secret sharing based visual cryptography scheme using CMY color space," *Procedia Computer Science*, vol. 78, pp. 563–570, 2015.

[10] A. Sherine and G. Peter, *A Novel Biometric Recognition System for FingerprintUsing Polar Harmonic Transform*, 2022.

[11] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, *Progressive Color Visual Cryptography*, School of Computing, National University of Singapore, 2003.

[12] S. K. Nerella, K. V. Gadi, and R. S. Chaganti, *Securing Images Using Colour Visual Cryptography and Wavelets*, International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[13] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, pp. 86–106, 1996.

[14] Z. Fu, Y. Cheng, and B. Yu, "Perfect recovery of XOR-based visual cryptography scheme," *Multimedia Tools and Applications.*, vol. 78, no. 2, pp. 2367–2384, 2019.

[15] S. Ahmad, M. F. Hayat, M. A. Qureshi, S. Asef, and Y. Saleem, "Enhanced halftone-based secure and improved visual cryptography scheme for colour/binary Images," *Multimedia Tools and Applications*, vol. 80, no. 21–23, pp. 32071–32090, 2021.

[16] J.-S. Pan, T. Liu, H.-M. Yang, B. Yan, S.-C. Chu, and T. Zhu, "Visual cryptography scheme for secret color images with color QR codes," *Journal of Visual Communication and Image Representation*, vol. 82, article 103405, 2021.

[17] Y. C. Hou, C. Y. Chang, and F. Lin, "Visual cryptography for color images based on color decomposition," in *Proceedings of the Fifth Conference on Information Management*, pp. 584–591, Taipei, 1999.