International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

A Novel Stack Based Visual Cryptography Scheme For Cover Images In Secure Communication Applications

R. Tamijetchelvy
Assistant Professor, Department of Electronics and Communication Engineering
Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India
tamilpkiet@yahoo.com

Abstract: Communication technologies have undergone a rapid evolution with the advent of state-of-the-art gadgets and transmission schemes. With increasing research in communication models aimed at fast and secure transmissions and receptions, the threat of hackers and malicious users have also grown exponentially. This has given rise to several security models aimed to conceal information being sent across channels in order to prevent unauthorized access and tampering of data in which cryptography is an integral part. Visual cryptography has gained significant importance in recent times due to its inherent merit of not requiring a complicated or dedicated decryption scheme at receiver end which greatly reduces the decryption time as well the computational complexity associated with it. A three-category cover image based stacked visual cryptography model is proposed in this paper and experimentations on visual decryption have been done indicating the merits of visual cryptography.

Keywords: Visual Cryptography**,** Cover Image Cryptography**,** Shares**,** Superimposition

I. INTRODUCTION

Rapid advancements in the field of information processing and communication technologies have led and motivated people to transmit more and more information across the globe irrespective of geographic location at a fast rate. Data privacy is a booming issue in recent times due to increased threat of data invasions by hackers, malwares etc. Traditional cryptography's encrypting approaches are commonly utilised for protecting information security. After the encryption is made, the data will be jumbled, which will be recovered by using the proper key. Even though unauthorised parties will steal the data, then the encrypted source content is hard to detect without the proper key.

The most striking aspect of the visual cryptography technique is that it is capable of recovering a cover message without involving any dedicated decrypting or decoding procedures [1]. The author [2] proposed Cover Image Share Embedded security algorithm (CISEA) to generate shares from the original image. The generation of compliment images of a cover image to which the secret shares are to be embedded. The threshold technique [3-5] allows for additional flexibility in the use of visual cryptography. A typical visual cryptography scheme is shown in Figure 1.

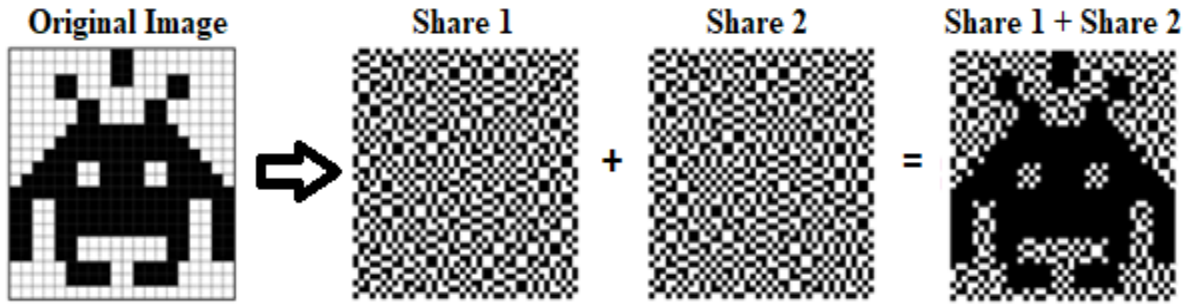

Figure 1. Illustration of concept of visual cryptography
[Courtesy: https://www.101computing.net/visual-cryptography/]

The challenge of secret sharing prompted the development of visual cryptography. One of the first difficulties to be explored in cryptography is secret sharing. A secret is separated into k pieces in an (n, k)-threshold issue. The secret can be properly reconstructed with any n of the k pieces, although even the entire knowledge of n-1 pieces does not provide any information about the secret. To tackle the (n, k) challenge, visual cryptography demonstrated a new paradigm. Based on the original image (the secret message), the original technique creates k images (called shares) that will be printed on k transparencies. As a result, anyone with no prior knowledge of cryptography can utilise a system based on visual

cryptography [6-9]. Each secret message is supposed to be indicated as a picture, and that the picture is simply a collection of white and black pixels, that is, it is considered to be a binary picture. Every original pixel is replicated in k modified representations of the picture (referred to as shares), one for each transparency. There are m white and black sub-pixels in every share. Each sub-pixel is printed near proximity on the transparency.

When the pixel in the original image is white, we refer to the built M as R0, and while the pixel in the original picture is black, we refer to it as R1. The scheme's most essential parameter is the number of pixels in a share. The resolution loss from the original picture to the restored picture is indicated by this parameter. The sub-pixel patterns in the shares for a white pixel are C0, and the sub-pixel patterns in the shares for a 1 pixel are black. With the rapid advancement of communication and computer technology, confidential information is increasingly being conveyed via the Internet. As a result, preventing secret information from being decrypted and suspected has become a crucial study topic.

Visual cryptography was originally introduced in 1994. Visual cryptography is a cryptographic technology that encrypts visual information (namely, handwritten notes, photographs, and printed text) so that it may be decrypted by the human visual system without the use of computers. The secret pictures may be restored using a stacking procedure, and the visual cryptography approach will reduce complex computation issues in the decryption process. Because of this quality, visual cryptography is particularly beneficial when only a lower computation load is required. With limited storage and bandwidth, two factors, the number of shares and the pixel expansion encoded, are important. The size of the share will be small as the pixel expansion is smaller in size.

When sharing numerous secrets, encoding numerous secret photos into a similar share image need little overhead. Because of the security difficulties over communication routes, meaningful shares will evade hacker notice. For example, in an (n, k) visual cryptography scheme, a dealer will encode a secret into n shares and provide a share for every participant, where every share will be transparent. If any n (or more) transparencies are stacked together, the secret will be seen; however, if the stacked transparencies are fewer than n, no secret information will be revealed. Private key management, conference keys, network auction, and multiparty computation are examples of applications for this method. Various confidential data is transmitted through the Internet, including commercial identifications and military maps. When using secret photos, security concerns should be considered, as hackers may take advantage of a weak link in a communication network to steal information. Various picture secret sharing techniques were created to address the security issues with secret photos.

This paper is organized as follows. Section 2 will discuss the related works. Section 3 proposes visual cryptography schemes in colour images. Then, the experimental results are reported. Lastly, the conclusion is given in Section 4.

II. RELATED WORKS

Many studies are made on visual cryptography [10]. However, most of them focused on discussing black and white pictures, with only a few proposing approaches to process grey-level and colour pictures. An existing method [11] suggested a visual cryptography technique to colour pictures. Every pixel of the colour secret picture is enlarged into a 2*2 block in this method, resulting in two sharing pictures. According to the approach, there are 24 possibilities of combinations based on the permutation of the four colours. The four-pixel colours are treated as average colour because the eyes of the human cannot identify the colour of a very tiny subpixel. Visual cryptography for colour images can be created easily by using this method.

Filling the blocks with green, red, white (transparent), and blue colours is not acceptable from the standpoint of either the subtractive or additive models of chromatology [12]. Another method [13] presented a colour picture sharing method. The technique starts by creating a secret image palette as well as assigning a unique code for every colour in the palette. Another method [14] offered a way to address the aforementioned problem. They employed binary encoding for indicating the subpixels chosen to every block, and the OR/ AND operation was performed at randomly for computing the binary code to each block's stacking subpixels in the cover pictures. The code goes from 0-255, but depending on the expanding factor, it can be considerably longer. As a result, a secret picture will be either true-colour or 256.

Another method [15] were able to share secret picture information to some extent, the problem is that secret images must be decoded using intensive calculation, which would violate the visual cryptography principle by using the eyes of the human for decrypting secret pictures. When these shares overlap, the hidden information is instantly revealed. Although, this technique does not require any mass processing to reassemble hidden pictures, it is nonetheless tough for obtaining complete random noise shares. On each sharing, certain image borders may be discovered, which compromises the required secrecy. An existing method [16] suggested a novel cryptography scheme known as Visual cryptography. Nowadays, the photos transferred on the web are primarily colour pictures. Visual cryptography needs to be expanded to include

colour images so that more data could be transferred, and more usage of visual cryptography algorithms could be utilised to ensure data security.

Another method offered three distinct algorithms for colour image visual cryptography [17]. cryptography, which will use HVS for decrypting the image without any cryptographic computation, but they are also entirely backwards compatible with every outcome which is already obtained in the research. Grayscale images can also be encoded using it. Many studies based on strategies that create meaningful shares have been conducted in order to avoid such shares. This approach [19] implemented and recommended a variation on the 2-in-1 picture secret sharing technique, where significant shares are produced and an authenticating picture is shared with the secret picture to ensure that no fraudulent shares are introduced.

III. PROPOSED WORK

A novel simple, yet efficient model of visual cryptography has been proposed and implemented in this paper based on generation of shares from R, G, B components of the input image sample. The general block schematic of the proposed work is shown below in Figure 2. It could be observed that the input image also known as cover image is subjected to certain preprocessing methods like contrast enhancement, filtering if the quality of the cover image is poor due to noise exposure, fading effects etc. this is followed by effective extraction of the red, blue, green components from which the shares are generated based on the method of thresholding.

The intensity values of images whose range is in the value of 0 – 127 are encoded with a 'one' while the values from 128 – 255 are encoded with a 'zero' thereby resulting in a binary image. Thus, a total of six shares are obtained for the three channels. In case of gray level images which has also been experimented in this work, two shares are generated per cover image.

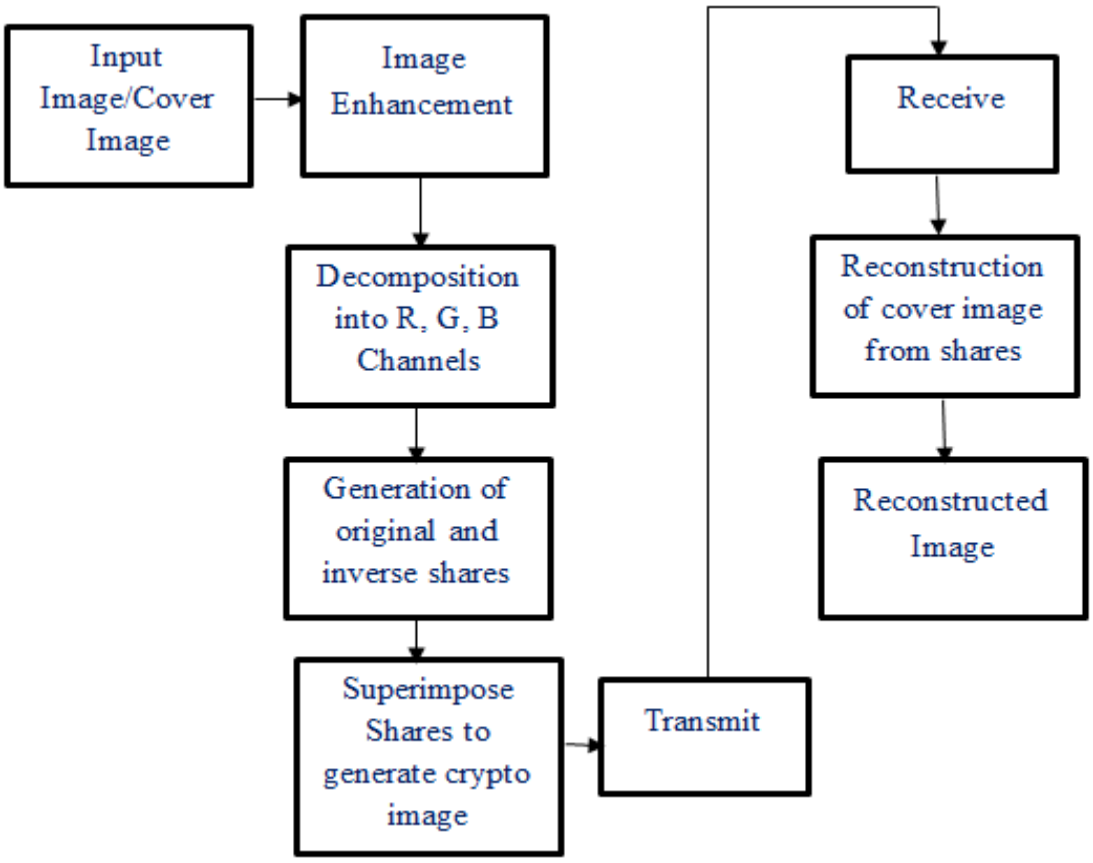

Figure 2. Illustration of proposed visual cryptography model

A pseudo code for this process is listed below

Input: Cover image I(x,y)
Output: Crypto image C(x,y)
Begin
{
While I(x,y)!=0.
{
For all x,y in I(x,y)
{

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

```
        R(x,y)|G(x,y)|B(x,y) = extract_channel(I(x,y))
        S1 = thresh_compute[R(x,y)|G(x,y)|B(x,y)]
        S2 = thresh_compute[R(x,y)|G(x,y)|B(x,y)]
        }
        For all S1and S2 of R(x,y)|G(x,y)|B(x,y)
        {
            S_impose [S1,S2] of R(x,y)|G(x,y)|B(x,y)
        }
    }
    End
}
```

IV. RESULTS AND DISCUSSION

The proposed stack-based visual cryptography model has been implemented in MATLAB environment running on an Intel 5 processor with 8GB RAM specification. Experimentation has been performed with three images namely color, gray scale and binary images to test the efficiency of the proposed model. The sample images taken for experimentation are shown below in Figure 3.

Figure 3. Illustration of the samples taken for experimentation a) Color image b) Grayscale image c) Binary image

Each of the three images have been experimented individually through the proposed stack based visual cryptography model. The shares along with cover image for color image is projected in Figure 4 shown below.

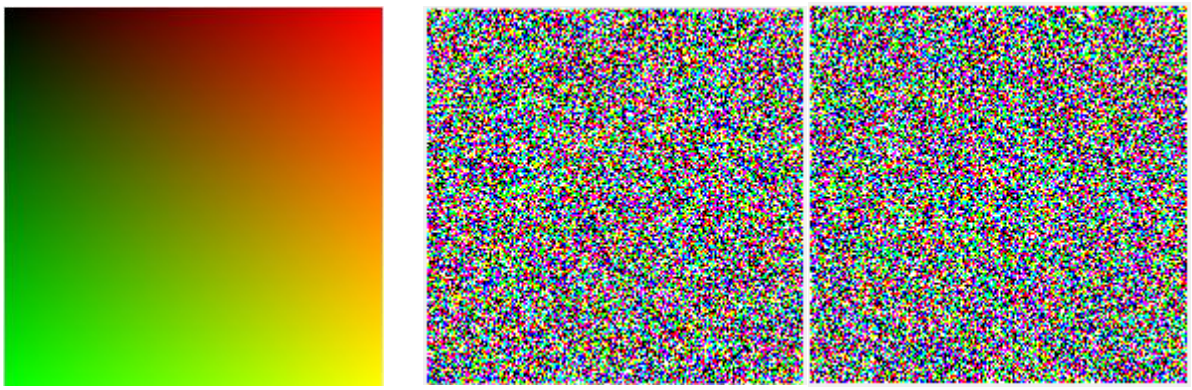

Figure 4. a) Cover image b) Secret share 1 c) Secret share 2

The encrypted shares are then transmitted to the receiver where the stacking of shares to be performed to obtain the decrypted image as shown in Figure 5. In this result without quality improvement and with quality improvement of decrypted images are illustrated for OR and XOR operation with the secret shares.

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 2 December 2020

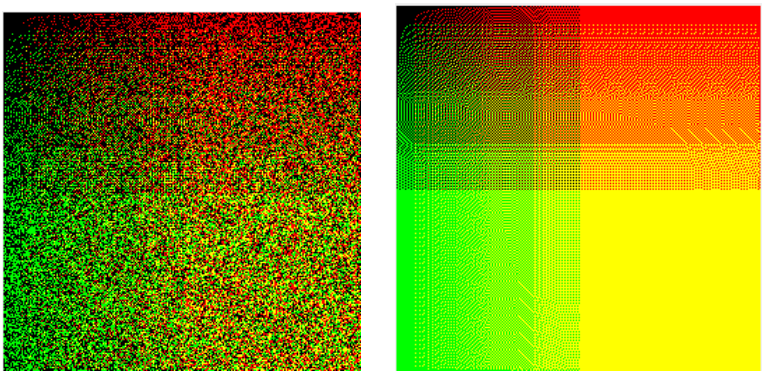

Figure 5. Illustration of Decyrpted Colour image a) Without quality improvement b) With quality improvement

A similar set of experimentation has been done with gray scale and binary images whose results are projected below.

Figure 6. a) Cover image b) Share 1 c) Share 2

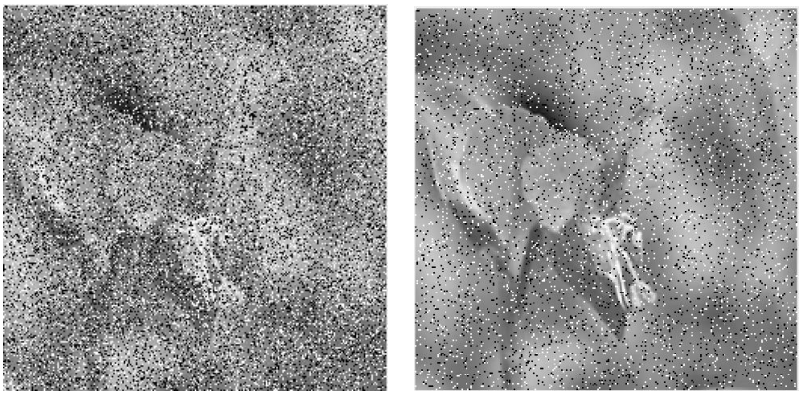

Figure 7. Illustration of Decyrpted Grayscale image a) Without quality improvement b) With quality improvement

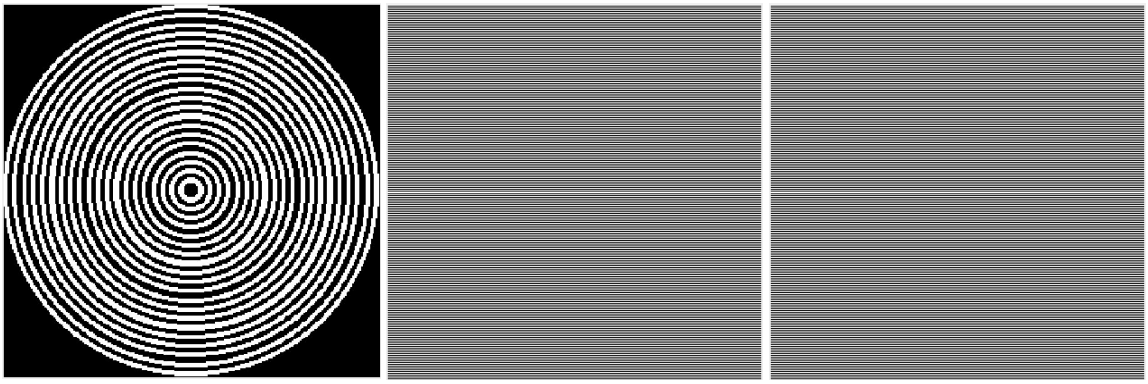

Figure 8. a) Cover image b) Share 1 c) Share 2

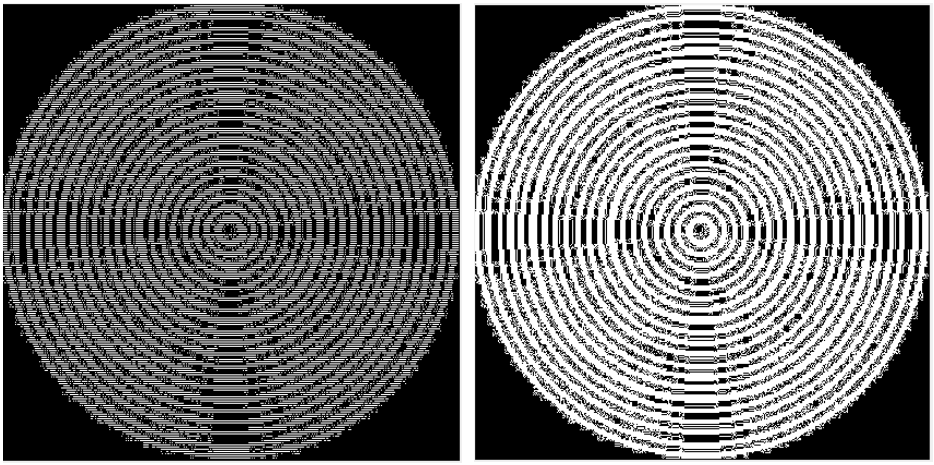

Figure 9. Illustration of Decyrpted Binary image a) Without quality improvement b) With quality improvement

It could be observed from the results that a near to perfect reconstruction is achieved in with quality improvement of XOR operation. The method is quite simple with no technical complexity and computational time overhead yet serves to be a simple but efficient method of delivering cryptic images with simple visual decryption at the receiver side

V. CONCLUSION

A simple stack based visual cryptography scheme has been proposed and implemented in this research work. Three samples of different categories namely color image, gray image and binary image have been taken as cover images to extract the shares and transmit them. In the receiver side, simple extraction of shares to reveal the cover image has been done. A small amount of noise is perceived in the decrypted images due to the additive noise components present in the channel. A simple XOR operation is performed to remove the noise and thereby enhance the image quality considerably. As a future scope of research, a frequency domain cryptography is thought of to make it closely resemble to be an invisible cryptography scheme.

REFERENCES

[1]. Wu, Xiaotian, Wei S. Extended capabilities for XOR-based visual cryptography. IEEE Transactions on Information Forensics and Security. 2014;9(10);1592-1605.

[2]. Sharma, Himanshu, Kumar, Neeraj, Jha, Govind Kumar. Enhancement of security in visual cryptography system using cover image share embedded security algorithm (CISEA). IEEE 2011 2nd International Conference on Computer and Communication Technology (ICCCT).2011; 462-467.

[3]. Prisco D. Roberto, Santis, Alfredo. On the Relation of Random Grid and Deterministic Visual Cryptography. IEEE Transactions on Information Forensics and Security. 2014; 9(4): 653–665.

[4]. Jena, Debasish, Jena, Sanjay Kumar. A Novel Visual Cryptography Scheme. IEEE 2009 International

Conference on Advanced Computer Control. 2009; 207-211.

[5]. Mugunthan, S. R. Soft computing based autonomous low rate DDOS attack detection and security for cloud computing. J. Soft Comput. Paradig.(JSCP). 2019; 1(02): 80-90.

[6]. Mandal J, Ghatak K, Subhankar. Constant aspect ratio based (2, 2) visual cryptography through meaningful shares (CARVCMS). IEEE 2011 International Conference on Communication and Industrial Application (ICCIA). 2011.

[7]. Sathesh, A. Enhanced soft computing approaches for intrusion detection schemes in social media networks. Journal of Soft Computing Paradigm (JSCP). 2019; 1(02): 69-79.

[8]. Yanyan, Han, Xiaoni, Cheng, Dong, Yao, Wencai. VVCS: Verifiable Visual Cryptography Scheme. IEEE 2011 Seventh International Conference on Computational Intelligence and Security (CIS). 2011; 974–977.

[9]. Sankaranarayanan, P, Tamijetchelvy, R, Gowthaman, R, Kumar, P. Compressive digital visual cryptographic scheme for multimedia application. International Journal of Applied Engineering Research. 2015; 20(10). 19176-19180.

[10]. Li S, Li J, Wang D. Region incrementing visual cryptography scheme with same contrast. Chinese Journal of Electronics. 2016; 25(4): 621-624.

[11]. Luo H, Chen H, Shang Y, Zhao Z, Zhang, Y. Color transfer in visual cryptography. Measurement. 2014; 51: 81-90.

[12]. Yang C. N, Tung T. C, Wu F. H, Zhou, Z. Color transfer visual cryptography with perfect security, Measurement, 2017; 95: 480-493.

[13]. Yan, Xuehu, Xin Liu, and Ching-Nung Yang. An enhanced threshold visual secret sharing based on random grids. Journal of Real-Time Image Processing. 2018; 14(1): 61-73.

[14]. Hou Y. C, Quan, Z. Y, Liao, H. Y. New designs for friendly visual cryptography scheme, International Journal of Information and Electronics Engineering.2015; 5(1).

[15]. Askari, N, Heys, H.M. and Moloney, An extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images. 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). 2013; 1-6.

[16]. Thomas, Sandhya Anne, Gharge, Saylee. Review on Various Visual Cryptography Schemes. IEEE 2017 International Conference on Current Trends in Computer.Electrical, Electronics and Communication (CTCEEC), 2017; 1164–1167.

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

[18]. Rola I, Khalid A, Randa, Dallah A, Aseel M. Al-Anani, Raghad Barham M., Salam I. Haji. A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes. Journal of Software Engineering and Applications.2017;10 (01):1-10.

[19]. Manasi AD, Deshpande R.V, Anti-phishing website using visual cryptography International Journal of Innovative Research in Computer and Communication Engineering, 2017; 5 (7): 13385-13393.

