



Enhanced Technique in VC With Four Meaningful Cover Images

Randa A. Al-Dallah¹, Aseel M. Al-Anani², Rola I. Al-Khalid³

¹Department Of Computer And Networks Engineering, Faculty Of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan, randa.dallah@bau.edu.jo

²Department Of Computer Information Systems, King Abdullah II School For Information Technology, The University Of Jordan, Amman, Jordan, a.anani@ju.edu.jo

³Department Of Computer Information Systems, King Abdullah II School For Information Technology, The University Of Jordan, Amman, Jordan, r.khalid@ju.edu.jo

ABSTRACT

Visual cryptography is an important technique for data hiding. In Visual cryptography (VC), a secret image is divided into multiple number of shares. Shares are distributed among multiple recipients, which makes it impossible for hackers to extract secret data from one share without having the other shares and thus data communication becomes secured. The secret data can only be disclosed by human eyes through stacking some or all of the shares. In this paper, we proposed a new image hiding technique that is based on VC. We embed a secret color image in four meaningful cover color images that have the same size as the secret image. The decryption method we used in our technique does not need previous knowledge of cryptography or complex computations thus maintaining the privilege of VC. The secret image can be retrieved if an acceptable number of cover images are stacked, otherwise; the original image retrieved may suffer from distortion and the required quality may not be achieved. According to our experimental results, our technique guarantees better quality of the retrieved secret image without pixel expansion and with less storage used as well as offering higher level of security.

Key words: Visual Cryptography, Encryption, Decryption, Meaningful Cover Image, Shares

1. INTRODUCTION

Nowadays, technology plays an important role in peoples' lives. The evolution of new technology affects different sectors such as education, industry, health, and data communication. It allows us to share data and information. On the other hand, valuable and sensitive data should be protected from unapproved access and hackers. Excess threats encouraged many researchers to be eager to find different methods to protect secret data so that any attempt to breach secrecy will result in a

complete failure. When discussing visual cryptography reference is made to Naor and Shamir. In 1994 [1], they proposed a secure and simple to implement method for sharing secret data. In their method, the secret black and white image is transformed into n shares, which are printed on separate transparencies and then distributed to n users. By overlapping k (or more) out of the n transparencies the secret image can be revealed. No information is gained if any $k-1$ transparencies are used. So decryption is performed by exploiting the human visual system without any complex computations which is an advantage that overcomes the disadvantage of pixel expansion where the size of the revealed secret image is not the same as the size of the original one. Several studies used visual cryptography as a security scheme for encrypting images in a simple way that can be later decrypted using vision [2] – [11]. Some studies concentrate on black and white images and others on color images [12][13][14][15][16].

Suzan proposed a new visual cryptography algorithm for colored image [17]. In her approach, she splits a 24-bit secret color image to number of shares. Each share contains part of the secret image. To generate these shares, the C, M and Y the reduction primitive color images are read in pixel by pixel and mixing OR operation together with $\frac{3}{4}$ pixel of cover image. According to the experimental results, it was found that the proposed method generated unclear and corrupted shares with noise. Moreover, they are easy to detect. So, she added some processing elements after recovery to improve color quality and generates an image similar to the original.

Hou, Quan and Tsia [18] developed a user friendly and unexpanded image sharing method based on the theory of progressive visual cryptography. They used four matrices (C_0-C_3) as the building blocks where each row of the matrix represents a possible way of sharing among n participants while each

column represents the information given to each participant. Four expandable dispatching matrices (M_0-M_3) each of size of $2n \times n$ were composed of C_0-C_3 to represent the four possible pixel combinations of the cover and secret images. According to their method, the dispatching matrices will not leak any secret information from the shadow image or the restored image. Besides, the quality of the restored images are improved. The recovered pixels in the black spots of the secret image are guaranteed to be fully black which gives better visual quality.

In order to get the best security performance, Karolin, Meyyappan and Thamarai[19] extends the visual cryptography basic model to the next level by using the Blowfish algorithm with 64-bit block cipher and creating a key with variable length in the range of 32-448 bits. In their approach, encryption and decryption processes are done using the Blowfish algorithm and the key. They used the Floyd-Steinberg dithering algorithm to manipulate the 256 color code images to reduce it to 16 standard color code images. They generate two shares of the secret image according to the traditional visual cryptography scheme where each pixel is expanded into 2×2 blocks arrays. Combining the two shares will generate the secret image without any complex computations.

In this paper, we proposed a new technique that is based on visual cryptography. We generate two meaningless shares from the secret color image. The two shares are then hidden in four meaningful color images. The secret image is revealed without any complex computation by superimposing the four cover images and exploiting the human vision system.

This paper is organized as follows. Section 2 presents the proposed method, section 3, discusses experimental results. Finally, some conclusions are given.

2. THE PROPOSED METHOD

We proposed a new hiding method that encrypts secret color image based on visual cryptography. In our method we used four meaningful cover color images (*CoverImage1*, *CoverImage2*, *CoverImage3* and *CoverImage4*) to hide one secret color image. All the images have the same size. The encryption method we used goes through two levels. The first level of encryption generates two meaningless share images (*Share1* and *Share2*) for the secret image using visual cryptography. The shares have the same size as the original secret image. The second level of encryption hides each share in two of the cover images. *Share1* is hidden and

embedded in the cover images *CoverImage1* and *CoverImage2*, while *Share2* is hidden and embedded in the cover images *CoverImage3* and *CoverImage4*. See Figure 1.

2.1 The First Level Of Encryption

This level undergoes several steps.

- ✓ **Step1:** The creation of the half toned image for the secret image using a dithering technique.
- ✓ **Step2:** The half toned image is split into three layers *Red*, *Green* and *Blue*.
- ✓ **Step3:** The generation of the two shares *Share1* and *Share2*.



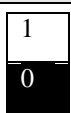
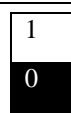
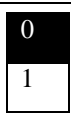
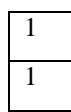

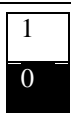

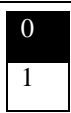
Each of the two shares, *Share1* and *share2* is composed of three layers. Each layer in the shares is a set of rows and columns that are filled randomly based on a private key.

To generate *Share1*, for each layer, the even rows are filled with zeros and ones randomly, while the odd rows are filled with the complement of the pixels above it in the even row. [20].

On the other hand, *Share2* is constructed based on *Share1* and the half-toned secret image as follows:

The layers of the shares and the half-toned secret image are divided into blocks of size 2×1 pixels. We start examining the corresponding blocks of *Share1* and the secret cover image two rows at a time. *Share2* is generated based on the following cases as shown in Table 1:

Table 1. Share2 block according to the corresponding Image block

Secret Image block	Share1 block	Share2 block
		
		
		
		

1	1	1
0	0	0
0	0	0
1	1	1

Case1: If the block in the secret color image is 0, 0 then the corresponding block of *Share2* will be filled with the complement of the values of the corresponding block of *Share1*.

Case2: If the block in the secret color image is 1, 1 then the corresponding block of *Share2* will be filled with the same values of the corresponding block of *Share1*.

Case3: If the block in the secret color image is 0,1 or 1,0, then the corresponding block of *Share2* will be filled with the same values of the corresponding block of the secret image taking into consideration that the corresponding block of *Share1* must also be the same otherwise fill *Share1* block with the same values of the secret color image.

The layers of both *Share1* and *Share2* after construction are combined to form *Share1* and *Share2*.

2.2 The Second Level of Encryption

In this level, *Share1* is hidden and embedded in the cover images *CoverImage1* and *CoverImage2*, while *Share2* is hidden and embedded in the cover images *CoverImage3* and *CoverImage4*. The embedding procedure is as follows:

For each pixel in *Share1* (which applies also on *Share2*) check the corresponding pixels in the two cover images *CoverImage1* and *CoverImage2* (or *CoverImage3* and *CoverImage4* in case of *Share2*). If the pixel in the *Share1* is 1, then the corresponding pixels in the two cover images must also be 1. If the pixel in the *Share1* is 0 and the corresponding pixels in the cover images are 0,1 or 1,0 or 0,0 then no changes are done and the corresponding pixels in the cover images remains the same. But if the corresponding pixels are 1,1 then in this case one of the cover images will set the pixel to 0.

At the end of this level, the two shares are hidden in the cover images. The cover images are meaningful but may suffer some slight distortion.

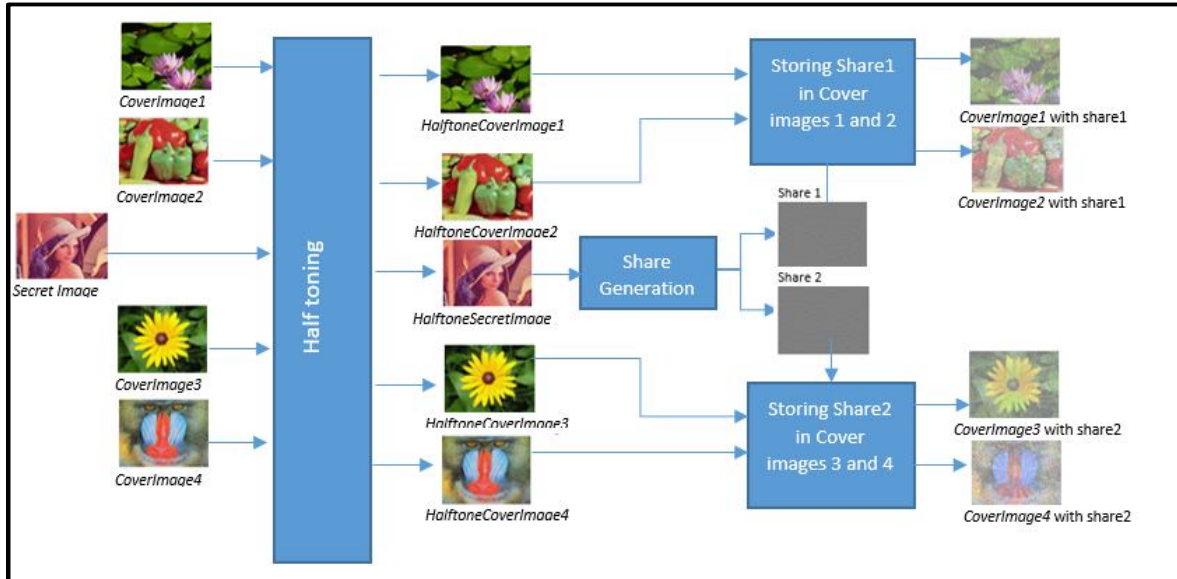


Figure 1. The encryption method

2.3 Decryption

At the receiving end, to obtain the secret cover image without any distortion, all what we have to do is to stack the four cover images without complex computations. As shown in Figure 2, superimposing the cover images in which the two shares are embedded will reveal the secret image at

the receptionist side without requiring any complex computation from his side. On the other hand, as shown in Figure 3, if any three of the cover images are stacked, we can obtain the secret image with slight distortion, this can be justified, since one of the cover images is not used where it holds part of one of the shares. Although not preferred, the secret

image can be recognized, if we use two cover images on condition that each of the cover images hides one of the shares (i.e. *CoverImage1* with *CoverImage3*, or *CoverImage1* with *CoverImage4* or *CoverImage2* with *CoverImage3* or *CoverImage2* with *CoverImage4*) but in this case the resulting secretimage will suffer from distortion. See Figure 4.

On the other hand, stacking the cover images that hides the same share (i.e. *CoverImage1* with *CoverImage2*, Or *CoverImage3* with *CoverImage4*) will result in having the share which does not give any information about the original secret image. See Figure 5.

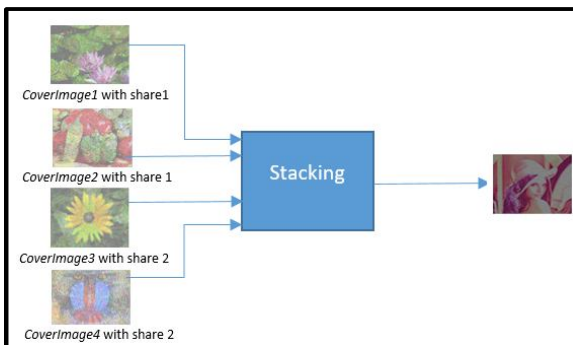


Figure 2. Stacking *CoverImage1*, *CoverImage2*, *CoverImage3* and *CoverImage4*.

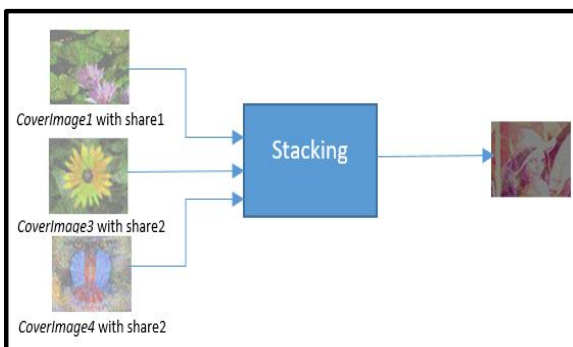


Figure 3. Stacking *CoverImage1*, *CoverImage3* and *CoverImage4*.

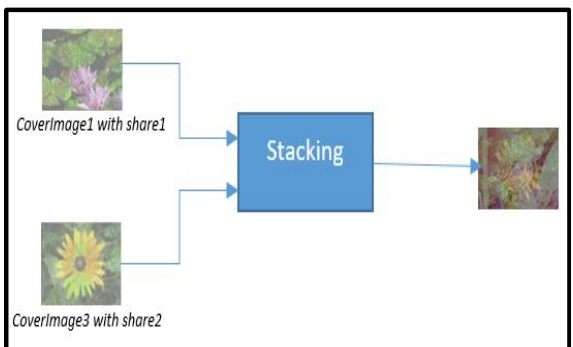


Figure 4. Stacking *CoverImage1* and *CoverImage3*.

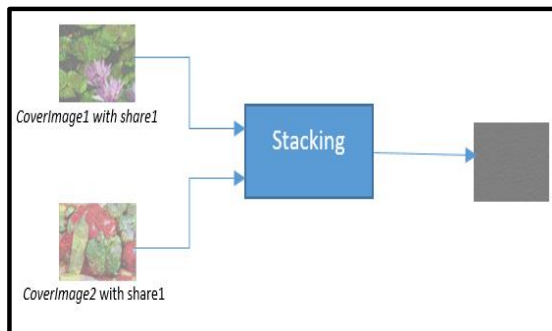


Figure 5. Stacking *CoverImage1* and *CoverImage2*.

3. EXPERIMENTAL RESULTS AND ANALYSIS

In order to check the validity of the proposed method, experiments have been conducted using five test color images. One for the secret image and four for the cover images. The test images are all of the same size 256×256 . The images are shown in Figure 6.

The generated two shares, *Share1* and *Share2* are also of the same size as in Figure 7.

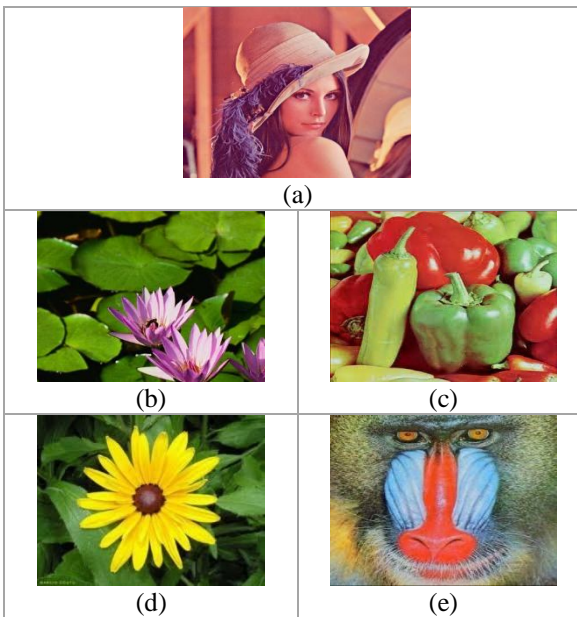


Figure 6. An example of the proposed method. (a) Color secret image. (b) *CoverImage1*. (c) *CoverImage2*. (d) *CoverImage3*. (e) *CoverImage4*.

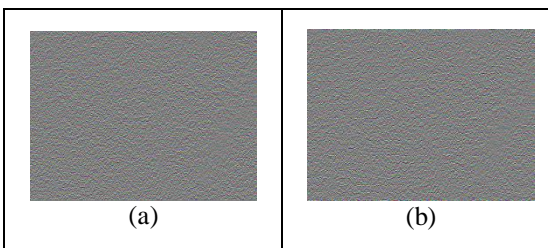


Figure 7. The two shares (a) *Share1*. (b) *Share2*.

The result of applying the second level of the encryption process is shown in Figure 8. *Share1* is hidden and embedded in the cover images *CoverImage1* and *CoverImage2*. see Figure 8 (a) and (b). *Share2* is hidden and embedded in the cover images *CoverImage3* and *CoverImage4*. See Figure 8 (c) and (d).

As can be noticed, the four meaningful cover images look so natural that any suspicion otherwise is dismissed.

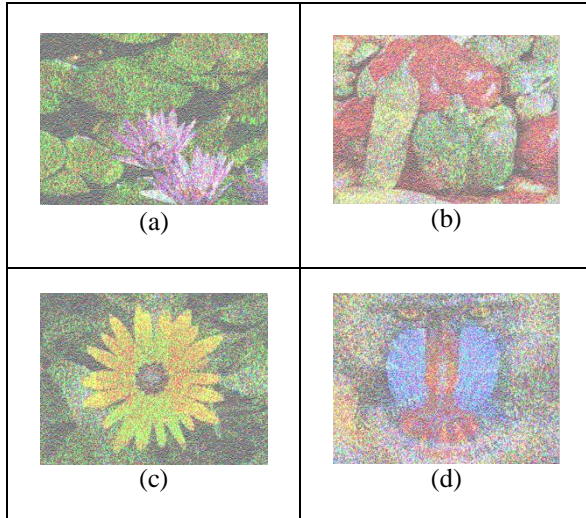


Figure 8. The four cover images after embedding procedure

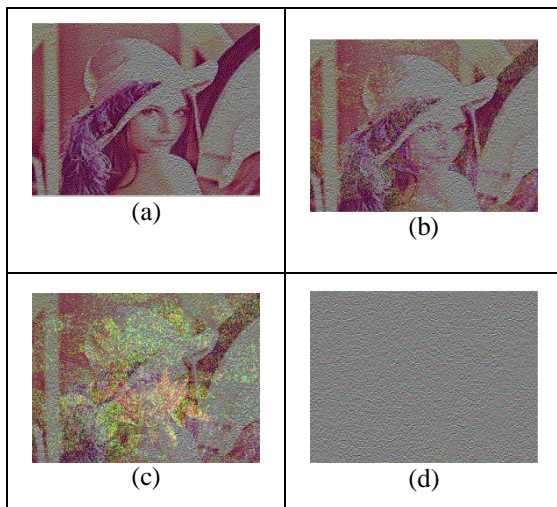


Figure 9. The Decrypted Image. (a) Stacking *CoverImage1*, *CoverImage2*, *CoverImage3* and *CoverImage4*. (b) Stacking *CoverImage1*, *CoverImage3* and *CoverImage4*. (c) Stacking *CoverImage1* and *CoverImage3*. (d) Stacking *CoverImage1* and *CoverImage2*

The experimental result that we conducted shows that our new method can successfully reveal the secret image by stacking the four cover images as shown in Figure 9(a). In Figure 9(b), the secret image suffers a slight distortion since only three out of four cover images are stacked. Stacking only two cover images hiding parts of *share1* and *share2* will not reveal the original secret image. Finally, stacking two cover images that hides the same share will result in having the share, which does not give any information about the original secret image. See Figure 9(d).

4. CONCLUSION AND FUTURE WORK

As technology is evolving rapidly and communication is becoming an essential part of our lives, the need for finding a secure way to transmit data has emerged. In this research work, we proposed a new image hiding technique that is based on VC. We embed a secret color image in four meaningful cover color images that have the same size as the secret image. The advantage of our technique is that the decryption process is based on a bit-wise AND operation which does not need previous knowledge of cryptography or complex computations. The secret image can be recognized if an acceptable number of cover images are stacked, otherwise; the original image retrieved may suffer from distortion and the required quality may not be achieved. All what we have to do to reveal the secret image is just by simply superimposing all or part of the cover images, many enhancements can be made to the proposed method such as generating meaningful shares because they look natural and do not draw hackers' attention.

REFERENCES

- [1] Naor, M. and Shamir, A. "Visual Cryptography". In: De Santis, A., Eds., *Advances in Cryptology—EUROCRYPT'94*. EUROCRYPT 1994. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. Vol. 950, 1995. <https://doi.org/10.1007/bfb0053419>
- [2] Kita, Naoki, and Kazunori Miyata, "Magic sheets: Visual cryptography with common shares.", *Computational Visual Media*, Vol. 4, No. 2, 2018, pp. 185+.
- [3] Sandhya Anne Thomas, and Saylee M. Garge, "Enhanced Security for Military Grid Reference System Using Visual Cryptography", *International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bangalore , 2018, pp. 1-7.

- [4] Thomas, S.A., danGharge, S., "Review on Various Visual Cryptography Schemes", In: 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). Mysore, India, 2017 pp. 1164-1167
- [5] K Brindha, N Jeyanthi, "Secret image enhanced sharing using visual cryptography", *Cybernetics and Information Technologies*, Vol. 17, No. 3, 2017, pp. 128-139.
- [6] Dua, R. and Singh, N., "Secured Visual Cryptography Scheme Using Meaningful Shares", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, 2016, pp. 5342-5347.
- [7] Ulutaş Mustafa, "Meaningful Share Generation for Increased Number of Secrets in Visual Secret-Sharing Scheme", *Hindawi Publishing Corporation*, Vol. 10, 1155, 2010, 1-18.
- [8] ArchanaB.Dhole and Prof. Nitin J. Janwe, "An Implementation of Algorithms in Visual Cryptography in Images", *International Journal of Scientific and Research Publications*, Vol. 3, No. 3, 1 ISSN 2250-3153, 2013, pp. 1-5.
- [9] Al-Anani, A.M., Abdallah, M.H., Al-Dallah, R.A. and Al-Khalid, R.I, "Multimedia Multilevel Hiding Technique", *European Journal of Scientific Research*, Vol. 24, No. 1, 2008, pp. 42-54
- [10] J. Tamilarasi, V. Vanitha, T. Renuka, "Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion", *International Journal of Scientific & Technology Research*, Vol. 3, No. 4, 2014, pp:126-131.
- [11] M. Sukumar Reddy, S. MuraliMohan, "Visual Cryptography Scheme for Secret Image Retrieval", *IJCSNS International Journal of Computer Science and Network Security*, VOL.14 No. 6, 2014.
- [12] KirtiDhiman and Singara Singh Kasana, "Extended visual cryptography techniques for true color images", *Computers & Electrical Engineering*, Vol. 70, 2018, pp. 647-658.
- [13] Varsha Hole, ApurvaNaik, RoshniPatil, Ankit Tiwari, "Visual Cryptography with Watermarking over Color Image", *International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2494-9150*, Vol 2, No. 01, 2016.
- [14] Manika Sharma, RekhaSaraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", *International Journal of Engineering and Innovative Technology (IJEIT)* Vol. 2, No. 10, 2013.
- [15] Al-Khalid, R., Al-Dallah, R. and Abdallah, M., "Efficient Techniques for Multimedia Information Hiding Using Color Visual Cryptography", *Dirasat: Pure Sciences*, Vol. 38, 2011, pp. 100-112.
- [16] H.-C. Wu, H.-C. Wang and R.-W. Yu, "Color Visual Cryptography Scheme Using Meaningful Shares", *Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications*, Vol. 3, 2008, pp. 173-178.
- [17] Sozan Abdulla, "New Visual Cryptography Algorithm For Colored Image", *Journal of computing*, Vol. 2, No. 4, 2010, pp. 21-25.
- [18] Young-Chang Hou, Zen-Yu Quan, and Hsin-Yin Liao, "New Designs for Friendly Visual Cryptography Scheme", *International Journal of Information and Electronics Engineering*, Vol. 5, No. 1, 2015, pp. 15-20.
- [19] Karolin, M.; Meyyappan, T.; Thamarai, S.M., "Encryption and decryption of color images using visual cryptography", *Int. J. Pure Appl. Math.* Vol. 118, No. 8, 2018, pp. 277-281.
- [20] Al-Khalid, R., Al-Dallah, R., Al-Anani, A., Barham, and R. and Hajir, S., "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes", *Journal of Software Engineering and Applications*, Vol. 10, No. 1, 2017, pp. 1-10.