Exploration of Color Visual Cryptography By Using Hybrid Technique

Khalid Akbar, Rao Sohail Iqbal, Ghulam Ali, Ume Aymen and Muhammad Yasir

Department of computer science, Government college university, Allama Iqbal Road, Faisalabad, Pakistan

Summary
To secure data is a vital part of communication and multimedia. To store and share data without having any access of third party is the real challenge. To avail this ability is an important art. A lot of method are being used recently in this regard. This may be done by converting a data into some unfamiliar forms, signals, or sketch etc. Which may not be read or understood by the third party. Cryptography is the best in this regard. Cryptography word has emerged from the Greek word Krypto hide and Grafo write .This technique has two methods encryption and decryption. The former deals with the conversion by possessing a key of fundamental data into unreadable form called encoding. Bringing of encrypted data into original form in decoding or decryption. We intend to put forward a private visual cryptography scheme that is robust and resilient enough to provide enhanced security of confidential information. In this paper, a comparison of the new hybrid visual cryptography scheme (HVCG) has planned enhance security and ensures secret image encryption completely private. An algorithm is quite dynamic, multi-level security by selecting the color of the random number implementation.

Key word:
Visual cryptography, Hybrid Cryptography scheme, Extended Visual Cryptography Scheme.

1. Introduction

Cryptography word has emerged from the Greek word Krypto hide and Grafo write. Its purpose is to protect the messages or characters be read.

Human history has occurred, because people have secrets, and other people want to know secrets. With pencil and paper is a first type of encryption and gain about this, they can easily acquire knowledge of staff. Password has been developed and it is very important of our daily life that safe our most vital data from unauthorized people.

Secure communications & encryption rules always provide privacy protection. A person's private life secret, commerce relationship, and to provide protection in all social or political activities secure communication of these conditions. Image may contain highly confidential and sensitive information. Profile picture sort used especially for military, scientific research office, solution advice, part of the regional government, sights and sounds, film and other sectors of the territory.

Their transmission, information can have obtained by the programmer and unauthorized clients for abuse and illegal work. These inconveniences usually happen in the communication network. Future information needs to be reliable, high amount of an insurance. Guarantee high insurance information's, passwords, it is reasonable to keep the system as a refuge as an information exchange. For the use of the fundamental purpose of encryption is to verify, mysterious, non-declaration, consistency and credibility of the exchange of information in any moment. Password can describe the ability of insurance documents, which ensures that the only stakeholders can has obtain. Internet information security has calculated atmospheric salient features. Information becomes more valuable for user other person, but it has also security issue. Cryptography is one of the largest information security in recognition technology. Visual cryptography was presented by Shamanic and Naor in 1994[1]. The image is separated into dissimilar chunks that is called parts. Stock transparencies readily available n stock will be spread to the participants of n. When all the parts are covered n unique images of the human eye to observe without any encryption method.

Encryption is the process of protecting personal information. Calculate it using some encrypted data, and then decrypted back by restoring real picture, that required the use of a secret key. We legacy encryption method is applicable to encrypted image, but there are 2 vital explanations remain illegal.

1: The traditional writing password images larger size requires a lot of time, real-encrypted image data.

2: Humanoid characteristics decrypted image consciousness is not necessarily equal to the original image of the image of small spin is appropriate, as long as people are able to observe changes and decryption written and unique writing basically the same.

These conditions humanoid graphics system is the most suitable and reliable way to do one covert retrieval. When the picture is divided or decomposed into N parts, they are equipped through top-secret sharing program if parts of N may amount to decrypt the image. It was through the N-1 shares can not disclose information to a single photo N shares covering the share of unique picture that can look the protection key and decrypt individual slide. The object

Manuscript received September 5, 2017
Manuscript revised September 20, 2017

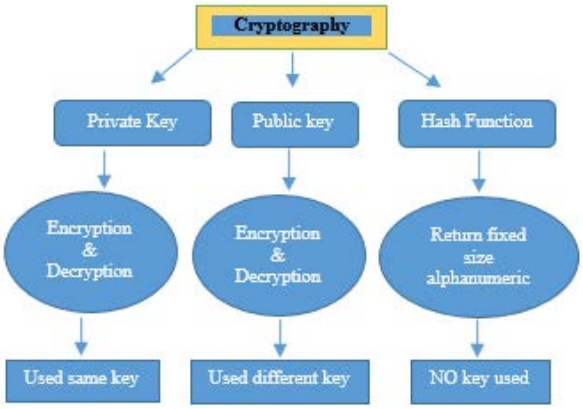
is to provide information security unit by super imposing visual application and use other encryption algorithm humble legacy encryption is present, most people use different methods complex. It is recognized (K, N) visual cryptography scheme ideal anywhere k represents the minimum amount necessary to decrypt the hidden parts of the image, n is VCS entire amount of stock taken

For color images on the 1st Venture pattern has been planned Verheul [2]. Visual cryptography scheme has been planned as bio-security, digital watermarking, information hiding. In web base system all the information is very important and hackers try to get these information and used it for its own purpose.

This technique has two methods encryption and decryption. The former deals with the conversion by possessing a key of fundamental data into unreadable form called encoding. Bringing of encrypted data into original form in decoding or decryption.

Cryptography is the ingenious process, so that mystery of the information. It is now re-learning or implied in some mysterious information checked. Cryptography is the picture content to ensure the best video communications equipment. Encryption abuse surveys hidden data and data puzzle.

Classification of Cryptography



2. Literature Review

In 1994 Shamir & Naor [1] presented Visual Cryptography, who explained the difficulty of encrypting written materials (such as text, notes). The decryption method requires only the human visual system (HVS) and does not need to be calculated. A late outline of visual cryptography has many program planed by Adhikari [3]. Blundo [4] eliminated the similarity of the visual encryption scheme of the plan with the best difference calculated in the basic matrix. They say that the optimal difference between n k and k is that k has a value of 4 or 5. Adhikari & Roy [3] planed a visual encryption scheme to get better results from pixel development Shamir & Naor. The Naor Shamir k in the VSC matches the k in the n VC, and the results show that their pixel development is less in all cases. Yang [5] planed another program that does not use white pixel frequency for pixel development to display contrast-improved images. Yang program can be easily applied to black and white visual encryption and pixel development. Due to the applicability of the black and white VCS program Verheul & van Tilburg [2] planned to obtain a faint picture from n visual cryptography. Several VCS schemes for grayscale images are proposed to solve these problems Chen [6].Lin & Tsai [7] has planned another visual encryption scheme for grayscale images. The grayscale image becomes a binary image with a similar size jitter, and then the Naor-Shamir's black and white image's visual encryption scheme is working. This scheme is a better growth of the pixel of the visual encryption scheme [2] and the pixel development speed is compared to Naor-Shamir's high contrast visual encryption scheme. Hou [8] first proposed three methods of encrypting color images. For the color VCS Hou program is the first set of color visual encryption schemes. He planned three previous procedures for grayscale and color images built in black-and-white VC halftones and color decomposition processes. Yang & Chen [9] used the modifier to mix the color of the modifier so that the improvement of the pixel subtracts the amount of shadow produced by the image in three ways, using the arrival frequencies of red, green and blue to simulate the secret color. The problem with this solution is that the only way to improve the color of its composition is to adjust the original image. Lukac & Plataniotis [10] proposed a color vision encryption scheme in 2005 that supports only two of the two arrangements and achieves pixel growth. Shyu [11] proposed a color vision encryption scheme in 2006. The Hyu scheme applied each of the n black and white visual encryption schemes to a picture that decomposes a unique concealed picture to support the whole of the n K. Hou & Tu [12] color vision encryption scheme supports k-sequence, no pixel growth. Jitter is required to preprocess the unique picture that has been hidden and the number of colors that are supported. Cimato [13] planned to solve the difficulties of most color-like pixels that cause color darkening at the expense of large pixel growth. By lowering the contrast quality to a certain level. Yang & Chen [14] proposed a color VCS scheme with a fixed pixel spreading factor of 3.Ateniese [15] planned the first k of n EVCS black and white pictures by using the hyper graph coloring process. Nakajima & Yamaguchi [16] have three plans. Input, and output is a shared image that is considered to be an input image. By covering two shared images, you can raise the third image. Wang [17] plan in n EVCS for gray and black pictures and EVCS plans for grayscale and color pictures. The basic condition of their scheme is to connect the basic matrix of the white and black image visual encryption schemes via the 2n

extension matrix. Wang main contribution program is to build an extension matrix. All of these programs have pixel extensions.

3. The Objective of the Study

The aim of our research is to provide proper security so that unauthorized users confidential information cannot be achieved. Our research focuses on improving the value of the output image through improved image contrast. Algorithm Related Sirhindi proposal EVCS image segmentation algorithm is divided into a red, green and blue halftone. Kandahar, who proposed using a random number to produce a peak into a number of sub-parts VCS program. Our technique is that all mixing of these two methods. The advantage of this program is Yes Safer and more dynamic and robust.

4. Algorithm to Encrypt and Decrypt the Image

Sirhindi proposed EVCS algorithm in a segmented image into red, green and blue halftone. Kandahar, who proposed using a random number to produce a peak into a number of sub-parts of the VCS solution. Our strategy is half and half approach of all these two.
Encryption algorithms:
Algorithm step are

1) Take picture as input
2) Distribution 256 valid secret key
3) Using a random number generator to select the colors
4) Using a random number of colors in the color picker to select randomly generated
5) The halftone image of the image in the selected color
6) Pass through the combination of a halftone image corresponding bit to build a sub-pixel block
7) Through selecting a number of pixels' transparent color fill in the blanks
8) Now, with some other image bit envelopes, and send
9) Monitor encrypted image effect

4.1 Decryption algorithms:

These step algorithms are.

1) Take the encrypted image input
2) Set aside 256 a mixture of the same secret key
3) Reads the encrypted image size
4) Bit image retrieval envelope
5) Split these bits to construct the same color halftone image
6) Pass through a combination of (or gate) of all halftone image original structure

4.2 Proposal mixing visual cryptography scheme

The recommendation mixing visual cryptography scheme in the literature, in order to ensure a more dynamic mix of secret sharing security and flexibility of the program mixing. The program has its roots in the previous program, and strengthen customer or user security and more powerful configuration secret sharing is an important application of the proposed technology until the time of computer communication or image hidden image.

Characteristic of the Hybrid visual cryptography scheme

The program combines Sirhindi Halftone Encryption [18] and VCS program by generating the number. The important nature of the proposed arrangement is accompanying.

1) Random number Color Creates a halftone image
2) It supports sub-pixel sub- group flexibility
3) Program follows the image of the envelope, to provide a more secure encryption
4) Subpixel minutes before the group to increase transparency bit
5) Decrypt a simple oring operation involves less computational burden

4.3 Encryption Properties

Encryption pre-programmed program involves a number of vector image of the original image by hiding. This process consists of the following important properties

1) For the n -first test of knowledge (also affects the color sub-pixels grouped and color names random number)
2) Random choice of colors, from a predefined list of colors
3) Creation halftone image from the original image
4) Half from each color forming sub-pixel group tone image
5) invert the subpixel bunches
6) These embedded image vector halftone image (the envelope)

4.4 Decryption properties

Secret image decryption by comprising the steps simple procedure.

1) For the n -first test of knowledge (number of colors)
2) Color name first test of knowledge (which create halftone)
3) Bit image support N + 1 of image segmentation (halftone + vector image)
4) Retrieving ň subpixel group ...

5) Combined with sub-pixel group and arrange reproduced halftone image
6) Reverse back to the sub-pixel to the original position
7) Halftone simple tone image oring to get the original picture

4.5 Flow chart program.

Complete program is shown in the following lines.

4.6 Encryption

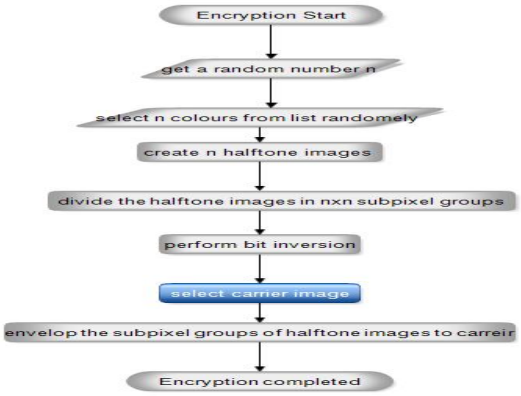


Fig.No.1.

VCG algorithm supports color images of all the encryption process does not require any hard and fast calculations. To hide the color image of many semi- color tone image processing is then split them further. All of these images further production in many sub-pixel groups, and then these groups of pixels in the image carrier enveloped. Inverted given more complex envelope hidden image before all the bits. Now, the image can be visually encrypted consideration.

4.7 Decryption

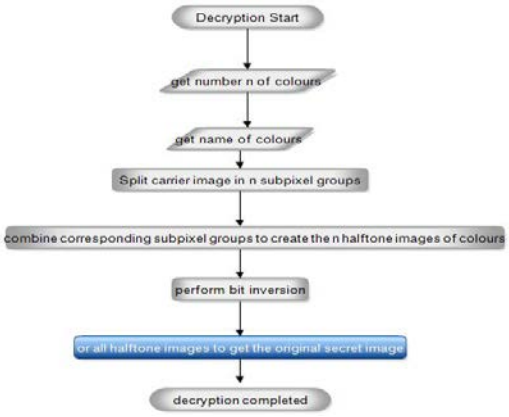


Fig.No.2.

Decryption process is simple yet critical programs. Existing knowledge is n and color names to making it more powerful and secure private. Then the received image is split into n x n sub-pixel group. In these groups, a halftone image is retrieved. To this end, according to all the sub-pixel group in order to obtain a halftone image and rearranged. Get to halftone before tone image, the sub pixels are inverted back to the group to obtain the original halftone image. Then, the halftone images being used or operated, to obtain the encrypted original image engagement.

4.8 The Hybrid Visual Cryptography scheme HVCG

Visual cryptography proposed plan would replace some of the necessary exhibition program. These programs integrate the use of any number of era []. Blackout encryption program focus of the investigation is the VC of color and black-level image halftone technology, white, black VC and color decomposition method based on the history of education. Our method preserves from the use of HVS information retrieval of video decoding / decryption black and white VC good place. The entire records of the investigation plan are given in the appended line.

4.9 Random number selection

The random number n is responsible for selecting the number of colors from the color list si []. CMY program Wang [18] used three fixed numbers of colors. Although the name of the color is also fixed in the same sense. Thus, random number generation can support a more robust structure in which a different number of colors can be selected.The number n additionally impacts the subpixel bunches. Subpixel bunch comprise of n x n pixels picked with a specific end goal to develop and wrapping picture for encryption. It can be an evident that a cut off on n must be important so that number choice and subpixel gathering ought to remain a legitimate gathering and effectively handle capable amid encryption.

4.10 Create a sub-pixel group

S image and n = 2. Randomly selected color split S1 and S2 Magenta and Cyan S.Then S is divided as S1 and S2. Wherein S1 represents the original image S transparent cyan image although S2 represents the original transparent products red image.
So that a pixel is disposed in the 2 × 2 mode. The following two moments of the case on behalf of the matrix

$$s_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$s_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

The chance of subpixel set might be

$$s_1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$s_2 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Or

$$s_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$$s_2 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

The formation of sub-pixels can have many other options group. For the above changes and orderly combination of columns of the matrix. Some other forces can replace the line as given below

$$\begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{O} & \mathbf{O} \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{1} & \mathbf{1} \end{bmatrix}$$

According to involve a lot of transparent images from the original color of the more secure encryption formation of selecting sub-groups. Examples are given of two colors assume the case. In the case of the order of two or more colors packet will be different.

These sub-pixel groups through a number of arrangements to mark their decryption program. Order sub-pixel group depends n the value. If n is 2, then the order will be 2 × 2 and N = 3 of the order will be 3 × 3 square matrices. This increases the more powerful in terms of encryption security. The dynamic nature of this matrix is formed in the decryption of adding more sense of unpredictability. If there is no prior knowledge of the probability of violation encryption tends to be low.

4.11 Bit inversion of pixel subgroups

Anti-bit transfer involves encapsulating inverted before pixel sub-group of bits. In the 2 × 2 square case of the array, bit reversal will o at 1 and 1 change to 0, for example, if the original rectangular array

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

The results of matrix after changing the bit inversion will be

$$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

The program applies more safely, to hide the safety of image encryption by hiding the original position. In the absence of inverting, a more strong security aspects, the image becomes a little bit feasible.

4.12 Selection of carrier image and enveloping scheme

Anti-bit turns to forward the image carrier selection algorithm. This is a vector image any image commands envelope process of pixel groups. If an image is formed on a transparent sub-groups are 2 × 2 so that it may in some 8 × 8 or 6 × 6-pixel group is shrouded. Check the applicability of a 8 × 8 pixel groups. Wherein the envelope successful execution.

Many of the proposed solutions in the literature Hou [20]. Through some carrying pictures of VCG a well laid out plan. VC method comprising a puzzle image into n film, in which each pixel is increased m times encrypted program, have been proposed NAOR & Shamir [1]. Mysterious pictures cannot be found from any outspoken, however, when K or higher transparencies screen together will begin to create a multi-faceted profound distinction between pixels' satisfactory opportunity, the human eye can see the picture of the puzzle.

Encrypted data and computational tools are not necessary to unlock method. This method is called (K, N) peripheral vision shared mystery. Now, the interpretation of the mysterious picture, suppliers arrange two n × m of scheduling grid (C0, C1), which address how to share and dull white pixels mysterious image, where n stay part numbers and m having a pixel level of progress. Without loss rearrangement, for the case we take case (K, N) = (2, 2). For this situation, each pixel on the mystery picture will be divided into two pieces, every 2 × 2 subpixel, two dim and two white centers inside.In a white pixel sharing, mentioning each piece of proposed content is the same sort, otherwise it is indispensable for sorting, and as shown in Table I shows

Although the pixel what value is mysterious picture is that each offer will appear as two physical and two dull white. Prosperity of the offer is the fact that the interceptor cannot find any information about a mysterious quote, make sure the light Blando [21] describes a method of packaging a number of pictures to transfer pictures.

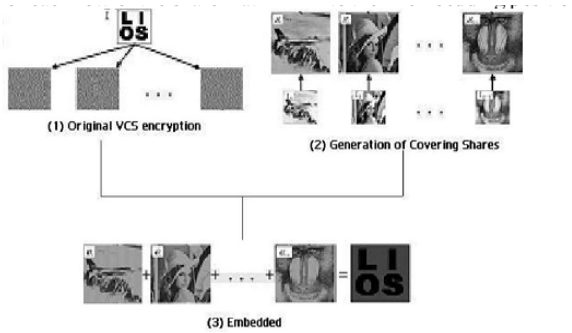


Fig.No.3.

The proposed scheme and the difference between this programs are the number of shares taken into account. HVCG scheme according to the following given the implementation process. Let some of the standard order of 6 × 6 in the carrier matrix given matrix of pixels

$$M1=\begin{bmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}$$

These are the 3 matrix

$$C1=\begin{bmatrix}0&0\\1&1\end{bmatrix}$$

$$C2=\begin{bmatrix}0&1\\0&1\end{bmatrix}$$

$$C3=\begin{bmatrix}1&1\\0&0\end{bmatrix}$$

The C_1, C_2 and C_3 rectangular array bit is inverted by the above procedure given to the formation of sub-pixel group. They can then in M1 enveloped in a certain position, it may be remembered retrieve them back matrix. The resulting carrier matrix will become

$$M1=\begin{bmatrix}0&0&0&0&0&0\\1&1&0&0&0&0\\0&1&1&0&0&0\\0&1&0&1&0&0\\1&1&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}$$

This can further send and enveloped matrix $Ç_1$, C_2 and C_3 from the same moment a position away from the identity matrix on the back of retrieval. Level results in the image surrounded by a large scene.

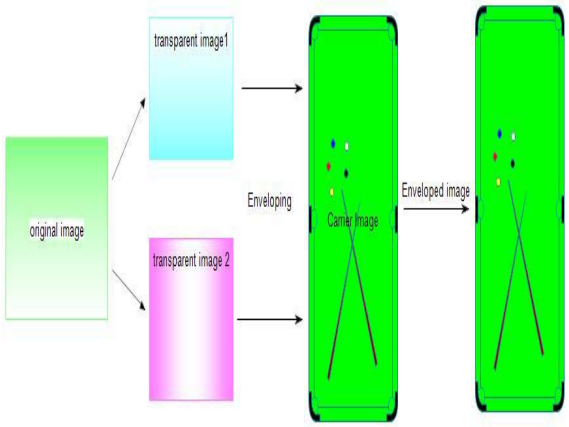


Fig.No.4.

This is the encryption diagram in which original image is divided in to two transparent. Both transparent envelope in to the carrier image and the send to the receiver.

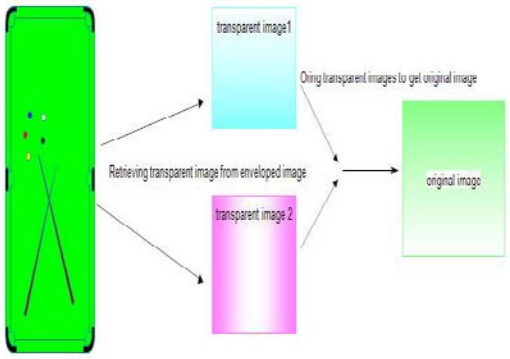


Fig.No.5.

This is the decryption diagram in which both the transparent image in come out from the carrier image and both the transparent combine make the original image.

5. Conclusion

This program used random selection shrouded in sub-pixel group composed of a halftone image of the image carrier. Envelope is a mixture of two pixels of the image to hide in a simple process of another image. This image is hidden operation sound and safe manner. By the envelope, the original pixel can be placed in a specific position of the

image carrier. Create a sub-pixel group before the first picture in a halftone image n isolated to ensure a more secure encryption. Halftone images are available in a single color is considered a concept of the original image layer. These single color choose from predefined colors random list. Color n is the random selection of predefined. All this process is robust, because of its dynamic random number selection. Also changes the number of colors of sub-pixel group is formed. This will bring the cost of processing, but it is simple, it will lead to the hidden images safer way. To improve the envelope prior to the completion of bit inversion encryption. The bit inversion system provide the full security in which all the 1 in the subpixel is convert in to the 0 and all the 0 in the sub pixel covert in to the 1.with this method only authorized person can get the real image.

References

[1] M. Naor and A. Shamir, Visual Cryptography, Advances in cryptology-, Lecture Notes in Computer Science pp. 1-12, 1994.

[2] E. R. Verheul, and H. C. Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes. Designs, Codes and Cryptography, vol.11. pp. 179-196, 1997.

[3] A. Adhikari, T. K. Dutta and B. A. Roy, new black and white visual cryptographic scheme for general access structures. In International Conference on Cryptology in India pp. 399-413, 2004.

[4] C. D. Blundo, P. Arcy, A. De Santis and D. R. Stinson, Contrast optimal threshold visual cryptography schemes. SIAM Journal on Discrete Mathematics, vol.16 pp. 224-261, 2003.

[5] C. N. Yang, New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters, vol. 25 pp. 481-494, 2004.

[6] C. S. Chan, Y. W. Liao, and J. C. Chuang, Visual secret sharing techniques for gray-level image without pixel expansion technology. Journal of Information, Technology and Society, vol. 95, 2004.

[7] C. C. Lin and W. H. Tsai, Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, vol.24 pp. 349-358, 2003.

[8] C. S. Hou and Y.C. Hou, Copyright protection scheme for digital images using visual cryptography and sampling methods. Optical Engineering, vol.44 pp. 077003-077003, 2005.

[9] C. N. Yang and T. S. Chen, colored visual cryptography scheme based on additive color mixing. Pattern Recognition, vol.41, pp. 3114-3129, 2008.

[10] R. Lukac, and K. N. A. Plataniotis, A cost-effective encryption scheme for color images. Real-Time Imaging, vol.11, pp. 454-464, 2005.

[11] S. J. Shyu, Efficient visual secret sharing scheme for color images. Pattern Recognition, vol.39, pp. 866-880, 2006.

[12] C. S. Hou and Y. C. Tu, Copyright protection scheme for digital images using visual cryptography and sampling methods. Optical Engineering, vol.44, pp. 077003-077003, 2005.

[13] S. Cimato, R. De Prisco and A. De Santis, Colored visual cryptography without color darkening. Theoretical Computer Science, vol.374, pp. 261-276, 2007.

[14] C. N. Yang and T. S. Chen, colored visual cryptography scheme based on additive color mixing. Pattern Recognition, vol.41, pp. 3114-3129, 2008.

[15] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures. Information and Computation, vol.129, pp. 86-106, 1996.

[16] M. Nakajima and Y. Yamaguchi, Extended visual cryptography for natural images, 2002.

[17] D. Wang, F. Yi, and X. Li, On general construction for extended visual cryptography schemes. Pattern Recognition, vol.42, pp. 3071-3082, 2009.

[18] R. Sirhindi, M. Afzal and S. Murtaza, an extended secret sharing scheme for colour images with fixed pixel expansion. International Journal of Electronic Security and Digital Forensics, vol.2, pp. 58-67, 2011.

[19] D. Wang, L. Zhang, N. Ma, and X. Li, two secret sharing schemes based on Boolean operations. Pattern Recognition, vol.40, pp. 2776-2785, 2007.

[20] Y. C. Hou, Z. Y. Quan and H. Y. Liao, new Designs for Friendly Visual Cryptography Scheme. International Journal of Information and Electronics, 2015.

[21] C. Blundo, A. De Santis and D. R. Stinson, On the contrast in visual cryptography s chemes. Journal of Cryptology, vol.12, pp. 261-289, 1999