International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Exploration of Color Visual Cryptography Schemes

Jinu Mohan[1], Dr. Rajesh .R[2]

[1]Research Scholar, Bharathiar University, Coimbatore, India

[2]Professor, Sree Narayana Gurukulam College of Engineering, Kadayiruppu, Kerala, India

Abstract: ***Secret sharing is a method for distributing a secret among a group of participants. Visual Cryptography is a form of Visual Secret Sharing proposed by Moni Naor and Adi Shamir. Visual Cryptography Schemes hide the secret image into two or more images which are called shares. The secret image can be recovered simply by stacking the shares together without any complex computation involved. Color Visual Cryptography encrypts a color secret message into color halftone image shares. In this paper the various Visual Cryptography schemes are discussed and try to summarize the recent developments in Color Visual Cryptography technology.***

Keywords: Visual Cryptography, Color Visual Cryptography, Halftone Technique, Color Decomposition.

1. Introduction

Information Security is an important aspect of present Internet computing environment. Information becomes more valuable when shared with others but it may also pose security issues. Hackers may try to access unauthorized data and misuse it. Hence various techniques of encryption have been developed to ensure secure transmission of information. Cryptography is one of the best known techniques for providing information security.

Visual Cryptography is a beautiful encryption technique for securing images and utilizes human visual intelligence as part of cypher algorithm. It is the pioneered work of Moni Naor and Adi Shamir, and was proposed in 1994 [1]. Here, an image is divided into different parts called shares. Shares are usually presented in transparencies. Each of the n shares will be distributed to n participants. When all the n shares are overlaid, the original image is visible by the human eye without any cryptographic technique. Any (n-1) shares will reveal no information about the original image.

The initial Visual Cryptography schemes were limited to black and white images only. The first Visual Cryptography scheme for colored images was proposed by Verheul and Tilborg in 1997 [2]. Visual cryptography schemes has been proposed for various applications like Biometric security, Watermarking, Steganography, Remote electronic voting, and User authentication scenarios.

This paper intents to provide an overview of initial visual cryptographic schemes and further compare some of the recent color VC techniques. This paper is organized into five sections. In section II, the various schemes of Visual Cryptography are discussed including some of the initial Color VC schemes. Techniques involved in relevant Color VC schemes are highlighted in section III. In section IV, comparison of recent color VC schemes has been described. Finally, the paper is concluded in section V.

2. Variants of Visual Cryptography

A. (2,2) Visual Cryptography Scheme

The original secret image is divided into two shares. Each share is printed in transparencies. By stacking the two shares, the original image can be reconstructed. No information can be revealed with any single share [1]. In Fig.1, Each pixel p is encoded into a pair of sub-pixels in each of the two shares. If a pixel p is white, the superimposition of the two shares always outputs one black and one white sub-pixel. If p is black, it yields two black sub-pixels. The superimposition of the shares represents the Boolean OR function. The decoded pixel is readily visible but there is a contrast loss in the reconstruction.

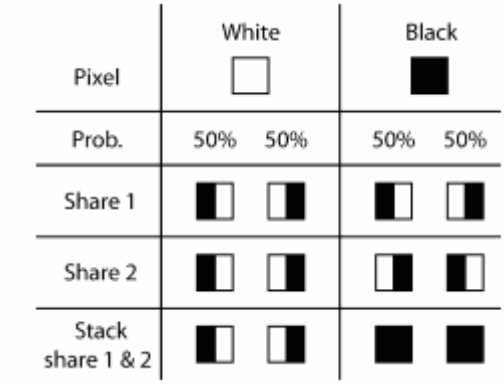

Figure 1: Construction of (2,2) VC scheme

B. (k,n) Visual Cryptography Scheme

The secret image is broken up into n shares which are distributed among n participants. Original image is visible by the human eye if k or more of these shares are stacked together, where the value of k is between 2 to n. The secret image will be invisible if the number of stacked shares is less than k [1].
It gives flexibility to the user. Any of the k shares are sufficient to decode the secret image. This in turn will reduce the security level of the system.

C. Size Invariant Visual Cryptography

R.Ito, H.Kuwakado, H.Tanaka presented the idea of Image Size Invariant Visual Cryptography (SIVCS) [3]. In SIVCS, the size of the transparencies are equal to that of the secret image. The concept of probability was combined with the Conventional Visual Cryptography scheme to generate a share of invariant size. They introduced a method suitable for binary images. Some authentication with steganography and cheating prevention schemes are used in SIVCS. Also

Visual Cryptography for color multiple secrets are emerging in this field.

D. Visual Cryptography Scheme for General Access Structure

An access structure is a specification of all qualified and forbidden subsets of n shares. Here, any k shares from qualified subset of shares can disclose the secret information. However, less than k shares even if from the qualified subset of shares cannot reveal any secret information. Even k or more shares from forbidden subset can't reveal secret information. This improves the security of the system [4].

E. Recursive Visual Cryptography

A 'Recursive Threshold Visual Cryptography' scheme was proposed by Abhishek Parakh and Subhash Kak [5]. The idea is that smaller secrets can be hidden in shares of larger secrets with secret sizes doubling at every step. So the information conveyed by every bit of share will be increased to nearly 100%. Recursive Hiding can be used to embed invisible watermarks, convey secret keys or encode authentication information. When used in network applications, the network load can be reduced. In this way, efficiency can be improved.

C. Extended Visual Cryptography For Natural Images

Extended Visual Cryptography is a kind of visual cryptography scheme in which meaningful shares are stacked together to reconstruct the original image. Mizuho Nakajima, Yasushi Yamaguchi proposed the EVCS scheme for natural images such as photographs [6]. This paper also focused on improving the quality of the output image by enhancing the contrast of the image. This is possible by extending the concept of error and by performing half-toning and encryption simultaneously. EVCS scheme can be applied in many real-time applications.

D. Halftone Visual Cryptography

Zhi Zhou, Gonzalo R. Arce, and Giovanni D Crescenzo proposed the concept of Halftone Visual Cryptography [7]. In this method, a secret binary pixel is encoded into an array of sub-pixels in each of the n shares. These sub-pixels are called as halftone cells. Visually pleasing halftone shares can be obtained by using halftone cells with an appropriate size. The halftone shares carry significant visual information to the viewers, such as landscapes, buildings etc. The above method can be applied in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash etc.

E. Color Visual Cryptography Schemes

Color Visual Cryptography encrypts a color secret message into color halftone image shares. In the color VC scheme introduced by Verheul and Van Tilborg, one pixel is distributed into m sub-pixels and each sub-pixel is divided into c color regions. In each sub-pixel, there is exactly one color region colored, and all the other color regions are black. The color of each pixel depends on the interrelations between the stacked sub-pixels. Disadvantage of the scheme is that the number of colors and the number of sub-pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will be a very difficult task. The method produces blocks with large numbers of black subpixels and visual quality of revealed image suffered.

Naor and Shamir proposed a color VC scheme in which a message is reconstructed with two colors by arranging the colored or transparent sub-pixels [8]. Here, a color is assigned to a sub-pixel at a certain position. The resulting pixels contain one colored sub-pixel and the rest of the sub-pixels are black. Disadvantage of the method is that the contrast of the images is reduced as more colors are used.

Rijmen and Preneel presented a scheme which enable multicolor with relatively less sub pixels [9]. However each sheet must contain color random images. So this approach cannot be applied to Extended Visual Cryptography.

To improve on the above method, Chang, Tsai and Chen proposed a new secret color image-sharing scheme based on the modified visual cryptography [10]. In this scheme, the secret image can be decoded precisely through a predefined Color Index Table (CIT) and a few computations. The recovered secret image has the same resolution as the original secret image in their scheme. However, as the number of colors in the secret image increases, the shares will also become larger. A major disadvantage is that additional space
is needed to store the Color Index Table.

F.Liu, C.K.Wu and X.J.Lin developed three new approaches for colored images based on Visual Cryptography [11].

1) In the first approach, colors in the secret image can be printed on the shares directly. Disadvantage is that it uses larger pixel expansion. This in turn leads to degradation of the quality of the decoded image.
2) In the second approach, three separate color channels are used. A color image is converted into black and white images on three color channels. Then the Visual Cryptography scheme for black and white images is applied to each of these color channels. Advantage of the method is that pixel expansion is reduced. However the quality of the image is degraded due to the half-toning process.
3) In the third approach, binary representation of the color of a pixel is used and the secret image is encrypted at the bit-level. Advantage is better quality of the image. Disadvantage is that it requires devices for decryption.

Pallavi Vijay Chavan and R.S. Mangrulkar presented a scheme using color Visual Cryptography for encrypting informative color image [12].

Firstly, various components are extracted from the input image. They are RED, GREEN, BLUE and ALPHA respectively. These components are used to generate the shares using 2 out of 2 secret sharing schemes. The secret information is divided into exactly two shares. One of these shares acts as a cipher text and other as a secret key. Each pixel in original is represented as a group of pixel in shares while generating shares. 4X4 pixel matrix is used in shares to represent a single pixel. Random combinations of horizontal pixels, vertical pixels or diagonal pixels are used for encoding of the original. Here the two shares are

generated in such a way that the pixel present in one share is not present on another share. These shares are superimposed together by performing X-OR operation. Thus the original image can be revealed. Advantage is that there is no expansion of the original image after encryption. The size of the revealed image after performing X-OR operation is exactly same as that of the original image. The reconstructed image contains negligible noise. This scheme can be extended to generate multiple shares instead of generating only two shares.

F. Progressive Visual Cryptography

In Progressive Visual Secret sharing scheme proposed by Jin, W. Q. Yan, and M. S. Kankanhalli, when more shares are stacked progressively, the recovery of the secret image will be clearer and clearer [13]. Only a sketch will be revealed when a few shares are being stacked and more details will be recovered when more shares are being stacked.

G. Image Hatching for Visual Cryptography

Image Hatching in general is a series of similar strokes which use various lengths, angles, mutual space and other properties of lines to represent parts of an image. These strokes give depth and shape to the image. Jonathan Weir and Wei-Qi Yan proposed a technique by which a secret can be hidden using visual cryptography within the hatched images [14]. This method can be used for image authentication. Generating these hatched images using a threshold based approach has proved to be very effective and easy to implement. One of the key strengths of the scheme is that it can take a multitude of images and apply these hatching styles to them. This type of secret encoding could have various potential secure applications particularly within the banking industry.

3. Relevant Color VC Schemes

Applying the technique of Visual Cryptography to color images is an important area of research since it allows the use of natural color images. Color images are also highly popular and have a wider range of uses when compared to other image types. Some of the relevant work on Color VC Schemes are discussed below:

A. Hou's Scheme

Young-Chang Hou developed an additive and subtractive model which is commonly used to describe the structure of colors [15]. Three primary colors red, green and blue (RGB) are used in the Additive Model. All the desired colors are obtained by mixing these RGB components. For calculating the intensity of red/green/blue components, the amount of red/green/blue in the compound light can be adjusted. The television screen is an example of the additive model. Fig 2 shows the additive model. In the Subtractive Model, color is represented by applying the combinations of colored-lights reflected from the surface of an object. This model use Cyan (C), Magenta (M) and Yellow (Y) color components and produce a wide range of colors. The color printer is an example of the Subtractive model. Fig 3 shows the subtractive model.

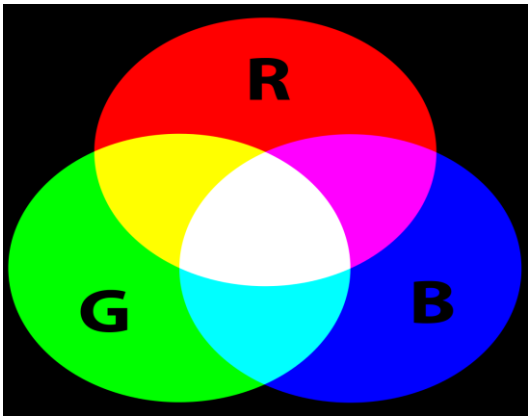

Figure 2: Additive model

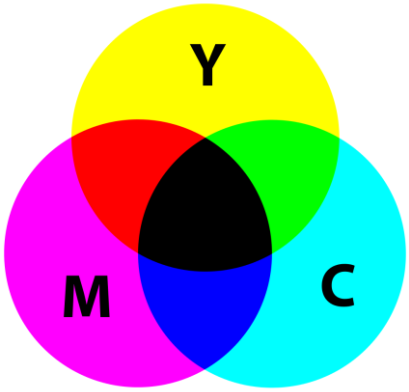

Figure 3: Substractive model

Hou's Scheme utilizes the principles of halftone technique and color decomposition. Halftoning is the process of using patterns of pixels of varying size and color to give the illusion of various shades. In this method, the color secret image is decomposed into three separate images that are respectively cyan (C), magenta (M) and yellow (Y). The three color images are translated into halftone images using the halftone technique. A color halftone image is finally generated by combining the three halftone images.

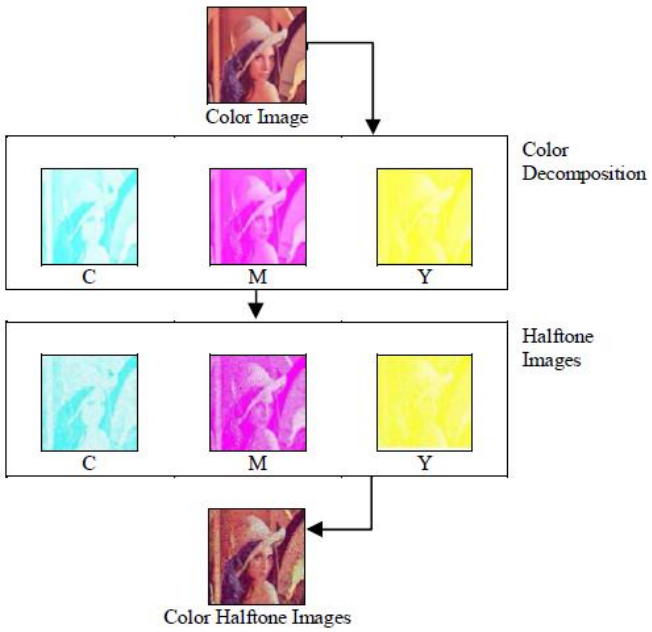

Figure 4: Color Decomposition for color halftone image

The color halftone image generation process is shown in Fig. 4. Disadvantage of this approach is that the shares generated using this technique is meaningless. These shares look like random dots. The looks of the meaningless shares reveals the existence of secrets to hackers.

B. Hsien-Chu Wu et al's Scheme

Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu developed a color Visual Cryptography scheme which produces meaningful shares [16]. In this method, two meaningful shares are generated using the halftone technique, cover coding table, and secret coding table.

Four different techniques are applied in the scheme:

(1) Color halftone transformation

The color image is transformed into a color halftone image. Two NXN cover images named CA and CB and NXN secret image SI are transformed into color halftone images CA', CB' and SI', respectively.

(2) Pixel Extraction Process

Some pixels are extracted from the color halftone image. For each halftone image generated, the pixels from the odd-numbered rows, or those from the even numbered rows, can be extracted out to make the extracted image. CA', CB' and SI' are pixels extracted to generate EA, EB and ES. In this way the size of the color halftone image can be reduced.

(3) Encoding

Cover images, named CA and CB are used to encode the secret image SI and thus two 2NX2N shares are generated. These shares are called Share1 and Share 2 respectively. Share 1 will be a meaningful share that looks just like CA. Share2 will be also a meaningful share that appears just like CB. In the encoding procedure, two coding Tables are used. Cover coding Table (CCT) is used for the encoding of the cover image. EA and EB is encoded using CCT. Secret Coding Table (SCT) is used for processing the extracted secret image. ES is encoded by the SCT.

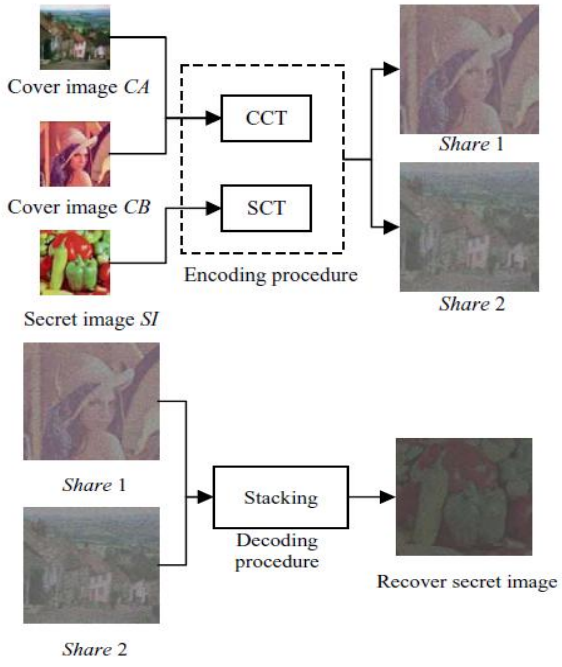

Figure 5: Encoding and Decoding procedures

(4) Decoding

The two meaningful shares generated are stacked together to recover the secret image. Fig 5 shows the encoding and decoding procedures of this method. Compared to Hou's scheme, this method provides more security. Since meaningful shares are generated, hackers are less attracted. A major advantage of the scheme is that only half of the pixels are needed to restore the secret image. This helps to save storage space in the main memory and the encoding time is also shortened. The strong encryption/decryption system also contributes to security. This scheme can be combined with digital watermarking or visual verification systems for practical applications.

C. Qin Chen's Scheme

Qin Chen, Xiarong Lv, Min Zhang, Yiping Chu proposed an Extended Visual Cryptography scheme for hiding multiple secrets [17].

In this method, meaningful shares are generated by contrast. The overlapping angle of meaningful shares can be changed for hiding multiple secrets. These steps can be applied to color images by utilizing halftone technology

There are four black-white images which are of size NXN. Two of these are considered as cover images and the other two are considered as secret images. The following five pixels should be considered in the process of encoding every pixel of the secret images: two pixels of cover images, the pixel of first cover image after its rotation and the pixels of the two secret images. So totally there will be 32 possible arrangement of pixels. Every pixel of the secret image is encrypted into a 3X3 block. The Hamming Weight of the block is the main factor which distinct the black and white pixel.

For applying the scheme to color image, the process of color division should be carried out initially. Every pixel is divided into 3 original colors: Red, Green and Blue. The continuous grey image with RGB channels is then transformed into a halftone image. The transformed halftone image can be dealt with the black-white Extended Visual Cryptography scheme. The color secret image will be revealed after the combination of the RGB shares.

The above method has a higher security level since the two shares generated are both meaningful images. The scheme is for multiple secret images. It extended from the application of black-white binary image to color images. So it has practical applications in the network environment. The above technique can be combined with digital watermarking or visual verification systems.

D. Deepa A K et al's Scheme

Deepa A K and Bento Benziger proposed an embedded EVCS scheme for color image using Artificial Bee Colony algorithm [18].

The secret image is converted into the CMY (Cyan-Magenta-Yellow) format. Then the shares are created using a dithering matrix. After that meaningful images are selected as cover images. The covering images are converted into CMY format and the half-toning technique is applied. Then

the covering images are divided into blocks and the shares are embedded on the covering images.

The following are the steps used for embedding shares on the covering images
Algorithm: The embedding Process
Step 1: Divide the covering image into blocks.
Step 2: Choose embedding positions in each block in covering images.
Step 3: Embed the sub-pixels on the covering image blocks. OR operation is the decryption technique used here for revealing of the secret image.

Artificial Bee Colony algorithm is used for the decrypted image to be better. This algorithm works similar to the behavior of bees in real life. Thus the visual quality of the recovered image is improved.

E. Meera Kamath et al's Scheme

Meera Kamath, Arpita Parab, Aarti Salyankar and Surekha Dholay proposed EVC scheme for color images based on Coding Tables [19]. As per the method the following techniques are used:

(1) Color Halftone Transformation

In this method, each input image is decomposed into three constituent planes red, green and blue. The principle of half-toning is applied to each of these planes. A color halftone image is generated by combining these three half-toned planes. Half-toning is performed using error diffusion. The error diffusion algorithm uses Jarvis filter. As per the Jarvis error diffusion algorithm, the error is diffused in the 12 neighboring cells. Visual quality of the half-toned image is higher when Jarvis algorithm is used.

Table 1: Analysis of relevant color visual cryptography schemes

Scheme	Year	No of Shares	No of Secret	Share Generation Method	Decoding Method	Type of Shares	Type of Color VCS	Security Level
Hou's Scheme	2003	2	Single	Halftone Technique, Color Decomposition	Stack the two shares together	Meaningless Shares	Color Visual Cryptography	Low
Hsien-Chu Wu et al	2008	2	Single	Halftone Technique, Cover Coding Table, Secret Coding Table	Stack the two meaningful shares together	Meaningful Shares	Color Visual Cryptography	High
Qin Chen et al	2010	2	Multiple	Principle of Contrast, Change the overlapping angle of shares	Stack the two shares together	Meaningful Shares	Extended Color VCS	Sufficient
Meera Kamath et al	2012	4	Single	Coding Table, Key Table, Jarvis Error Filter	Stack two or more shares along with the key image	Meaningful Shares	Extended Color VCS	High
Deepa A K et al	2014	2	Single	Dithering Matrix	Stack the shares using OR operation	Meaningful Shares	Embedded Extended Color VCS	High

(2) Encoding and Generation of Shares

A Key Table and two types of Coding Tables are used for encoding the secret image into the cover images. Key Table is used for key generation process. A Cover Table is used for encoding of the cover image. Secret Table is used to encode the pixels of the secret image. The encoded cover images are meaningful shares. So they can be transmitted securely. The sender has the option to select two or more of the four shares generated for transmission.

(3) Decryption

Two or more shares are stacked along with the key image to reconstruct the secret image. Using the Key Table guarantees that the pixels of the secret image are encoded in different ways. Any share by itself, or a single share along with the key image will not reveal the secret image. The Key Table and the Image Encoding procedure used considerably improves the security by increasing the randomness. High visual quality is achieved using this method.

Disadvantage is that the size of the shares produced and the final image after stacking are twice the size of original image.

4. Analysis

In this paper various color VC schemes are studied and their performance is evaluated based on some criteria like share generation, number of secret images, decoding method etc. In Hou's method based on halftone technique and color decomposition, the shares generated are meaningless. These shares look like random dots. To improve on Hou's technique, Hsien-Chu Wu et al developed a method to produce meaningful shares. He used two coding tables and the half-tone technique. This method also has a strong encryption/decryption system. Qin Chen et al developed an Extended Visual Cryptography scheme for hiding multiple secrets. Traditional Visual Cryptography suffers from share identification problem. This problem can be solved by Extended Visual Cryptography scheme in which a meaningful cover image is added in each share. This scheme is very easy and effective and security level is improved. Meera Kamath et al used a Jarvis error filter and two coding tables for encoding and generation of shares. The visual quality achieved by this method is higher compared to the previous schemes. and effective and security level is improved. Random shares are embedded onto meaningful

covering shares in Embedded Extended Visual Cryptography scheme. In this scheme for color Image proposed by Deepa A K et al, the visual quality of the recovered image is higher using Artificial Bee Colony algorithm. Table 1 shows comparison of various color VC schemes.

5. Conclusion

Visual Cryptography is the current area of research where a lot of scope exists. This interesting encryption technique is now being used by several countries for secure transfer of handwritten documents, financial documents, internet voting etc. In this paper, recent developments in color Visual Cryptography Scheme has been discussed. A comparative study has been conducted to analyze the techniques involved in Color Visual Cryptography. Integrating Visual Cryptography Scheme with digital watermarking or steganography could lead to potential number of applications.

References

[1] M. Naor, and A Shamir, "Visual Cryptography," Proceeding of Euro crypt 94 Lecture Notes in Computer Science, LNCS963, Berlin: Springer, pp1-11 (1994).
[2] E. R. Verheul, and H.C.A. Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs, Codes and Cryptography, 11(2): pp 179-196, (1997).
[3] R. Ito, H. Kuwakado, H. Tanaka," Image size invariant visual cryptography", IEICETrans. Fundam. Electron. Commun. Comput. E82-A (10)(1999)2172-2177.
[4] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, "Visual cryptography for general access structures", Proc.ICAL96,Springer,Berlin,1996,pp.416-428.
[5] Abhishek Parakh and Subhash Kak "A Recursive Threshold Visual Cryptography Scheme", CoRR abs/0902.2487: (2009).
[6] Nakajima, M. and Yamaguchi, Y., "Extended visual cryptography for natural images" Journal of WSCG. v10 i2. 303-310.
[7] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521-52.
[8] M. Naor, and A Shamir, "Visual Cryptography II: Improving the Contrast via the CoverBase," In Proc. of Security protocols. international workshop 1996, Lecture Notes in_Computer Science No. 1189, Springer-Verlag, pp 69-74, (1997).
[9] V. Rijmen, and B. Preneel, "Efficient Color Visual/Encryption for Shared Color of Benitton, 'Eurocryp' 96, Rump Session, Berlin, 1996, Availableathttp://www.iacr.org/conferences/ec96/rump/preneel.ps.
[10] C. Chang., C. Tsai, and T. Chen, "A new scheme for sharing secret color images in computer network," Proceedings of International Conference on Parallel and Distributed Systems, 2000(7), pp 21-27, (2000).
[11] F. Liu, C.K. Wu, X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.
[12] Pallavi Vijay Chavan, R.S.Mangrulkar, "Encrypting Informative Color Image using Color Visual Cryptography", Third International Conference on Emerging Trends in Engineering and Technology, pp 277-281,2010.
[13] Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, pp. 1-13, 2005.
[14] Jonathan Wier, Wei-Qi Yan, " Proceedings of International Conference on Machine Vision and Image Processing",2009.
[15] Y. C. Hou, "Visual Cryptography for Color Images," Pattern Recognition,2003,(36),pp1619-1629,(2003).
[16] Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu, "Color Visual Cryptography Scheme Using Meaningful Shares" Eighth International Conference on Intelligent Systems Design and Applications, pp-173-178,2008.
[17] Qin chen, Xiarong Lv, Min Zhang,Yiping Chu, "An Extended Color Visual Cryptography Scheme with Multiple Secrets Hidden",International Conference on Computational and Information Sciences, pp521-524,2010.
[18] Deepa A K, Bento Benziger, "Embedded Extended Visual Cryptography Scheme for Color Image using ABC Algorithm",Proceedings of International Conference on Signal Processing,pp 653-657,2014.
[19] Meera Kamath, Arpita Parab, Aarti Salyankar, Surekha Dholay, "Extended visual Cryptography for Color Images Using Coding Tables" , International Conference on Communication, Information & Computing Technology, pp1-6, Oct. 19-20,2012.