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.

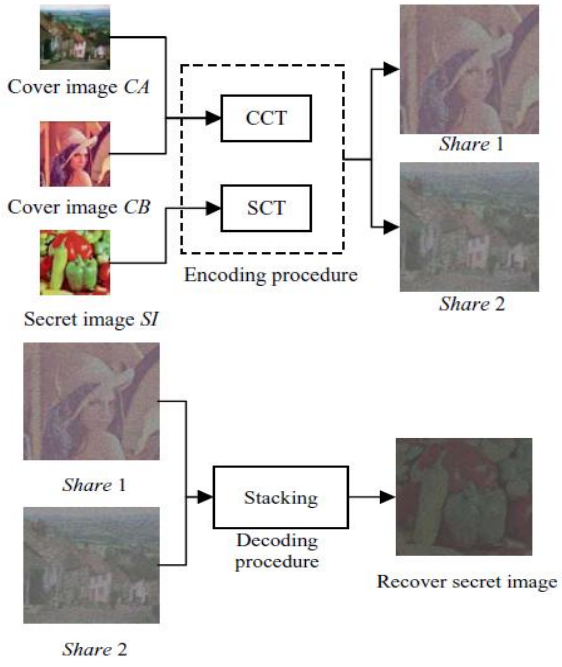

Figure 5: Encoding and Decoding procedures

(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.