Copyright Assurance Scheme for computerized Color Images Utilizing Key based Visual Cryptography Watermarking

P. Pardhasaradhi
Associate Professor, CSE,
Bapatla Engg. College
Bapatla, Andhra Pradesh, India

P. Seetharamaiah, PhD
Professor, CSSE,
A.U. College of Engineering,
Visakhapatnam, India,

Prasad Reddy P. V. G. D, PhD
Professor & Head, CSSE,
A.U. College of Engineering,
Visakhapatnam, India

ABSTRACT
With rapidly growing network, Internet has turned into an essential wellspring of transmitting confidential or secret data, for example, military data, money related records, and so forth. In such cases, strategies committed to ensure such kind of information are needed and they play an imperative role in providing confidential and secure transmission over network. Visual cryptography scheme is a cryptographic strategy which allows visual information to be encoded in such a way that the decoding can be performed by the human visual system, without the guide of PCs. In this article, it is proposed that a copyright assurance scheme for computerized color images utilizing key based Visual Cryptography Watermarking to accomplish the requirements of robustness and security. The master share is encoded with a copyright image to form another share called proprietorship share. The master share is kept with a central authority and possession share is kept by the copyright proprietor. In case of any dispute, the master shares and proprietorship shares can be stacked together to give the copyright image confirming the possession about the host picture. The imperative feature of this technique is that it will not disturb the host image either during copyright generation nor during copyright check. At long last, trial comes about demonstrate that the proposed plan can oppose a few basic assaults.

Keywords
watermarking, secret sharing, visual cryptography, copyright protection, image processing.

1. INTRODUCTION
With rapidly growing network, Internet has turned into an essential wellspring of transmitting confidential or secret data, for example, military data, money related records, and so forth. The encoding advancements of conventional cryptography are normally used to ensure information security. With such technologies, the information become disordered after being encrypted and can then be recovered by a right key. Without the right key, the encrypted source content can hardly be detected even though unauthorized persons steal the data. Naor and Shamir [1] proposed a new cryptography area, visual cryptography, in 1994. The most outstanding feature of this approach is that it can recover a secret image without any computation. It abuses the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography. The threshold scheme [1, 2, 5] makes the application of visual cryptography more flexible. With the k out of n threshold scheme ($k \leq n$); the manager can first produces n copies of transparency drawn from the secret image, one for each of his members. If any k of them stacks their transparencies together, the substance of the secret picture will appear. If the quantity of transparencies is less than k, the substance of the secret image will remain hidden.

There have been many published studies [1-6] of visual cryptography. Most of them, however, have concentrated on discussing black-and-white images, and just few of them have proposed methods for processing gray-level and color images. Rijmen and Preneel [7] have proposed a visual cryptography approach for color images. In their approach, each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. Rijman and Preneel [7] claimed that there would be 24 possible combinations according to the permutation of the four colors. Because human eyes cannot detect the color of a very tiny sub-pixel, the four-pixel colors will be treated as an average color. When stacking the corresponding blocks of the two shares, there would be 24^2 variations of the resultant color for forming a color image. The approach of Rijmen and Preneel indeed can produce visual cryptography for color images. But from the viewpoint of either the additive model or the subtractive model of chromatology, it is not appropriate to fill the blocks with red, green, blue, and white (transparent) colors. Besides, if we use the average of the four-pixel colors in the stacking blocks to represent the corresponding pixel color in the original image, the problem of circular permutations occurs. Since two circular permutations of a stacking block are not considered different, two average colors with different permutations will be the same in the stacking block if they have the same combination. Hence the number of possible color variation is fewer than the authors claimed 24^2.

Recently, Chang et al. [8] proposed a color image sharing technique. The algorithm first creates a palette of a secret image and assigns a unique code to each color on the palette. It then selects two colored cover images, O_1 and O_2, with sizes the same as the secret image. Every pixel in the two cover images will be expanded into a block with $M(= k \times k)$ sub-pixels, of which $\lfloor M/2 \rfloor + 1$ sub-pixels are randomly selected and filled with the color of the expanded pixel and the rest are filled with white (transparent) color. The selection condition is that N positions of the two expanded blocks are overlapped, where N is the index of the palette of the secret image and is used to indicate the pixel color shared by the two expanded blocks. When recovering the secret image, the algorithm computes the number of the overlapping sub-pixels of every $k \times k$ block in the two camouflage images and then

retrieves the N^{th} color from the palette to reconstruct the color of the corresponding pixel of the secret image. But this method can only deal with a color image with limited different colors. For example, if k equals 3, $\lfloor M/2 \rfloor + 1$ is at most 5, which is obviously too small and unreasonably restrictive for today's applications.

Hou et al. [9, 10] proposed a method to improve the above drawback. They used the binary encoding to represent the sub-pixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking sub-pixels of every block in the cover images. The code ranges from 0 to 255, but it can be even larger depending on the expanding factor. Consequently, a secret image can be a 256 color or true-color one.

Although Chang and Hou et al. [8–10] achieved a certain degree of sharing color image information, the drawback is that secret images must be decrypted with heavy computation, which would violate the principle of visual cryptography that uses human eyes to decrypt secret images.

Hou et al. [11] used the concepts of color decomposition and contrast adjustment to produce two shares needed by visual cryptography. Overlapping these two shares will reveal the secret information automatically. Although this method requires no mass computation to reconstruct secret images, it is nonetheless difficult to obtain totally random noise shares. Some image boundaries might be found on each share, thus compromising the secrecy required.

In this work, we will combine the previous results in visual cryptography, the halftone technology, and the color decomposition principle to develop algorithms of copyright protection scheme for computerized color images. Our method retains the advantage of traditional visual cryptography, namely, decrypting secret images by human eyes without any cryptography computation. For information security, it also ensures that hackers cannot perceive any clue about the secret image from any individual sharing image.

The rest of this paper is organized as follows. In section 2, we will introduce the concept of Visual Cryptography (VC), Color Models, and Error Diffusion for those readers, who are not familiar to it. Then, the proposed scheme is introduced in section 3. In section 4, we will demonstrate some experimental results to prove the robustness of our scheme. Finally, conclusions are given in section 5.

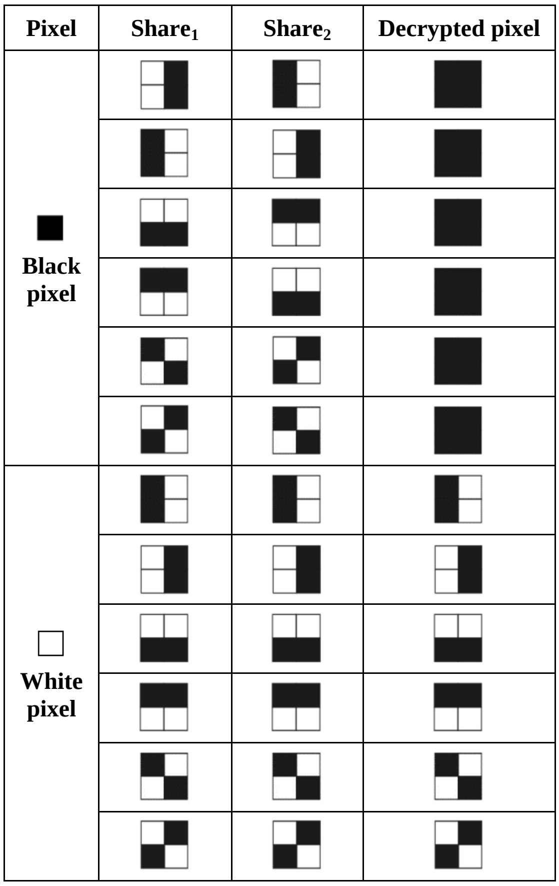
2. PRELIMINARIES

In this section, we give a brief description of VC, color models in VC and an error diffusion quantization. For more details about these topics, refer to [1], [2], and [3].

2.1 Introduction to Visual Cryptography

Visual cryptography is a powerful technique which combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics introduced by Naor and Shamir [1]. In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into shares of random binary patterns. The shares are Xeroxed onto transparencies, respectively, and distributed amongst participants, one for each participant. No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any transparencies together. The secret cannot be decoded by any $k-1$ or fewer participants, even if infinite computational power is available to them. VC scheme proposed by Naor and Shamir [1] serves as a basic model and has been applied to many applications. Aside from the obvious applications to information hiding, there are many applications of VC, which include general access structures [4], copyright protection [12], watermarking [13], [14], visual authentication and identification [15], print and scan applications [16], etc.

Table 1 Construction of $(2,2)$ VC scheme: a secret pixel is encoded into four Sub-pixels in each of two shares. The decrypted pixel is obtained by superimposing the blocks in shares one and two.



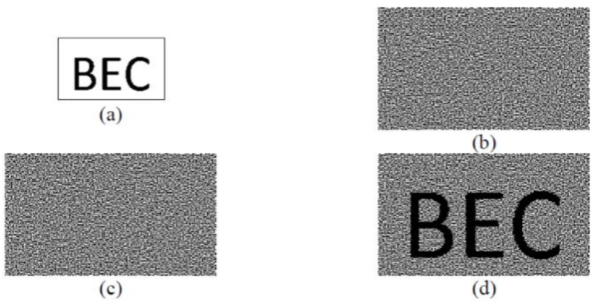


Figure 1. Example of 2-out-of-2 scheme

To illustrate basic principles of VC scheme, consider a simple $(2,2)$-VC scheme in Table 1. Each pixel from a secret binary image is encoded into black and white sub-pixels in each share. If is a white (black) pixel, one of the six columns is selected randomly with equal probability, replacing. Regardless of the value of the pixel, it is replaced by a set of four sub-pixels, two of them black and two white. Thus, the sub-pixel set gives no clue as to the original value of. When two sub-pixels originating from two white are superimposed, the decrypted sub-pixels have two white and two black pixels.

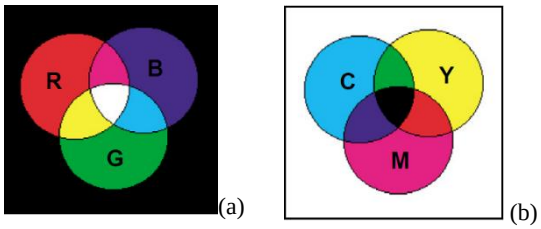
On the other hand, a decrypted sub-pixel having four black pixels indicates that the sub-pixel came from two black pixels.

Figure 1 shows an example of a simple $(2, 2)$-VC scheme with a set of sub-pixels shown in Table 1. Figure 1(a) shows a secret binary message, Figure 1(b) and 1(c) depict encrypted shares for two participants. Superimposing these two shares leads to the output secret message as shown in Figure 1(d). The decoded image is clearly identified, although some contrast loss is observed.

In a k-out-of-n VSS scheme (or called (k, n)-threshold VSS scheme), the secret is visible only when at least k or more shares are stacked together. Therefore, a VSS scheme is suitable for group secret sharing without the help of a computer. A VSS scheme is constructed for an access structure, $(\Gamma_{Qual}, \Gamma_{Forb})$, which specifies how the secret is shared among n participants. Suppose there are two participants, i.e. $P = \{1, 2\}$. Further suppose the qualified set is all the subsets of P containing at least two participants and all remaining subsets of P are forbidden. The family of qualified sets is $\Gamma_{Qual} = \{\{1, 2\}\}$, and the family of forbidden sets is $\Gamma_{Forb} = \{\{1\}, \{2\}\}$. Participants belonging to a qualified set can see the secret through stacking their transparencies together, and those belonging to a forbidden set cannot perceive any information from the stacked image.

2.2 Color Models

The additive and subtractive color models as shown Figure 2 are widely used to describe the constitutions of colors. In the additive color model, the three primary colors are red, green, and blue (RGB), with desired colors being obtained by mixing different RGB channels. By controlling the intensity of red, green, blue channels, we can modulate the amount of red, green, blue in the compound light. The more the colors are mixed, the more the brightness of the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model. In the subtractive model, color is represented by applying the combination of colored-lights reflected from the surface of an object. By mixing cyan, magenta and yellow pigments, we can produce a wide range of colors. The more the pigments are added, the lower the intensity of the light is and, thus, the darker the light is. This is the reason it is called the subtractive model. Cyan, magenta, and yellow are the three primitive colors of pigment which cannot be composed from other colors. The color printer is a typical application of the subtractive model and, hence, the VC model of Naor and Shamir is also of such kind.



(a) (b)

Figure 2. (a) additive and (b) subtractive color models

2.3 Error Diffusion

Error diffusion [17] is a simple yet efficient way to halftone a gray-scale or color image. The quantization error at each pixel is filtered and fed into a set of future inputs. Figure 3 shows a binary error diffusion diagram where $f(m, n)$ represents the pixel at (m, n) position of the input image. $d(m, n)$ is the sum of the input pixel value and the diffused errors, $g(m, n)$ is the output quantized pixel value. Error diffusion consists of two main components. The first component is the thresholding block where the output is given by

$$g(m,n) = \begin{cases} 1, & if\ d(m,n) \geq t(m,n) \\ 0, & otherwise. \end{cases}$$

The threshold $t(m, n)$ can be position dependent. The second component is the error filter $h(k, l)$ where the input $e(m. n)$ is the difference between $d(m, n)$ and $g(m, n)$. Finally, we compute $d(m, n)$as

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l)\, e\,(m-k, n-l)$$

where $h(k, l) \in H$ and H is an $2 - D$ error filter. A widely used filter is the error weight originally proposed by Floyd and Steinberg

$$h(k,l) = \frac{1}{16} \times \begin{bmatrix} & \cdot & 7 \\ 3 & 5 & 1 \end{bmatrix}$$

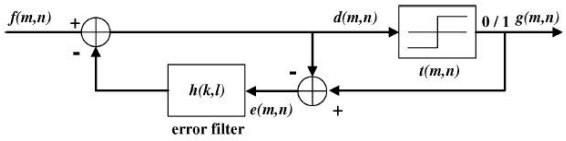


Figure 3. Error diffusion block diagram

2.4 Pseudorandom Number Generator

Pseudo random numbers are the output of a deterministic algorithm which is used to produce the numbers which must look like a random sequence and should satisfy all the criteria of randomness and the probability of occurrence of any number from the universe of numbers has an equal chance of being chosen [19]. Cryptography and randomness are closely related. Perfect secrecy can be achieved if the key is secure, according to Kirchhoff's Principle guessing the key should be so difficult that there is no need to hide to encryption/decryption algorithm. Secrecy can be achieved if the key of the encipherment algorithm is truly a random number. A Pseudo-Random Bit Generator (PRBG) is a deterministic algorithm which, given a truly-random binary sequence of length n, outputs a binary sequence of length $l(n) > n$ which appears to be random, with $l(n)$ being a polynomial. The input to the PRBG is called the seed, and the output is called a pseudo-random bit sequence [20]. A pseudo-random number generator uses this approach.

3. PROPOSED SCHEME

In this section, it is proposed that a copyright protection scheme for color images based on VC [18]. Essentially, the scheme comprises the ownership registration and the ownership identification phases as shown Figure 4. In the ownership registration phase, the master share M will be generated from the host image. Then, the master share M is used together with the secret image S to generate the ownership share O according to some predefined encryption rules of VC. During the process of randomized transposition, a private key K is used so that the identical sequence of pixel values can be drawn out from the host image in both phases. Finally, the private key K is kept in secret by the copyright owner, and the ownership share O must be registered with a trusted third party for further authentication. When a controversy over the ownership of the host image happens so that the copyright owner wants to prove his or her rightful

ownership, the ownership identification procedure should be performed. Thus, the private key K and the ownership share O are used to reveal the hidden secret image for settling the dispute. In the following sections, we describe our scheme in more detail.

3.1 Ownership Registration Phase

Assume that a copyright owner wants to hide a bi-level secret image S of size $N_1 \times N_2$ pixels into a color host image of size $M_1 \times M_2$ pixels for protecting his or her ownership. In the beginning, transform the color image into halftone image of C, M, and Y in advance. In addition, a private key K should be used for sampling so that a list of random numbers, $L = (l_1, l_2, \dots)$ can be generated by a pseudorandom number generator seeded by K, where each random number $l_m \in \{1,2, \dots M_1 \times M_2\}$ corresponds to the location of a pixel in the host image. Then each pixel m_{ij} of the master share M can be generated by the following generation rules.

Table 2. Encryption rules

Secret image pixel	Host image	Master share sub-block	Ownership share sub-block	Revealed Image sub-block
□	(0,0,0)			
	(1,0,0)			
	(0,1,0)			
	(0,0,1)			
	(1,1,0)			
	(0,1,1)			
	(1,0,1)			
	(1,1,1)			
■	(0,0,0)			■
	(1,0,0)			■
	(0,1,0)			■
	(0,0,1)			■
	(1,1,0)			■
	(0,1,1)			■
	(1,0,1)			■
	(1,1,1)			■

Now, we can start to generate the ownership share. Assume that s_{ij} denotes a pixel of the secret image$S$, and o_{ij} denotes a pixel with 4 sub-pixels of the ownership share O. Then, the resultant master share M is used together with the secret image S to generate the ownership share O according to the Table 2 generation rules.

Figure 4. Proposed Copyright assurance scheme

Algorithm ownership share construction procedure

Input: A color host image H with $M_1 \times M_2$ pixels, a bi-level secret image S with $N_1 \times N_2$ pixels, and a private key K.

Output: An ownership share O of size $N_1 \times N_2$ pixels (each of which is composed of 4 sub-pixels)**.**

Step 1: Transform the color host image H into halftone image of C, M, and Y

Step 2: Generate a list of random numbers $L = \{l_1, l_2, \dots\}$, where $l_m \in \{1,2, \dots, M_1 \times M_2\}$, by a random number generator seeded by K.

Step 3: select $n(n = N_1 \times N_2)$ pixel values $x_1, x_2, \dots, x_n$ from the host image H (according to L)

Step 4: For each pixel s_{ij} of the secret image S and pixel x_i from the host image of above sequence determine the color of the pixel o_{ij} (with 4 sub-pixels) in the ownership share O according to the Table 2 encryption rules.

Step 5: Repeat steps 3 to 4 until all pixels of the secret image S are processed.

Finally, the private key K must be kept secretly by the copyright owner for proving his or her ownership, and the

ownership share O should be registered with a trusted third party for further authentication**.**

3.2 Ownership Identification Phase

In the Internet era, it is very possible that a digital image is held or abused without the permission of the copyright owner. When a controversy over the ownership of the image happens so that the copyright owner wants to prove his or her rightful ownership, the ownership identification procedure should be performed accordingly. In the ownership identification phase, the copyright owner should provide the same private key K used in the ownership registration phase so that the correct sequence of pixel values can be obtained during the sampling process. Then, the master share M' is generated from the controversial image H' by the following algorithm.

Algorithm master share construction procedure

Input: A color host image H' with $M_1 \times M_2$ pixels, an ownership share O of size $N_1 \times N_2$ pixels (each of which is composed of 4 sub-pixels), and a private key K.

Output: A Master share M' of size $N_1 \times N_2$ pixels (each of which is composed of 4 sub-pixels)**.**

Step 1: Transform the color host image H into halftone image of C, M, and Y

Step 2: Generate a list of random numbers $L = \{l_1, l_2, \dots\}$, where $l_m \in \{1,2, \dots, M_1 \times M_2\}$, by a random number generator seeded by K.

Step 3: select $n(n = N_1 \times N_2)$ pixel values $x_1, x_2, \dots, x_n$ from the host image H' (according to L)

Step 4: For each pixel x_i from the host image of above sequence determine the color of the pixel m_{ij} (with 4 sub-pixels) in the master share M' according to the Table 6.3 encryption rules.

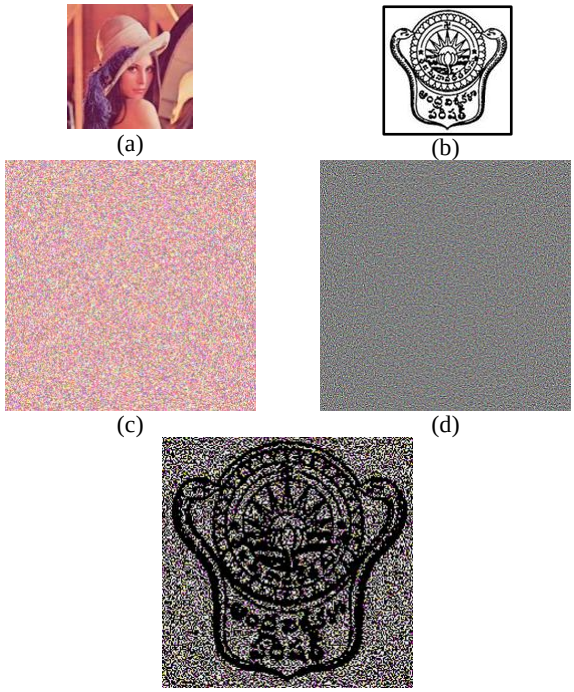
Step 5: Repeat steps 3 to 4 until n pixels of the H' (according to L) are processed.

After the master share M' is created, the secret image S can be revealed by visual cryptography. it can be simply printed both shares onto transparencies and then superimpose them to reveal the secret image without the aid of computers.

4. EXPERIMENTAL RESULTS

The color host image H of size 512×512 pixels is shown in Fig. 5(a) and the bi-level secret image S of size 256×256 pixels is shown in Fig. 5(b). The master share M generated from the original image is shown in Fig. 5(c), the corresponding ownership share O is shown in Fig. 5(d), and the stacked result of Fig. 5(c) and Fig. 5(d) is illustrated in Fig. 5(e).

We simulate some common attacks on Fig. 5(a). We use the PSNR (peak signal-to-noise ratio) to represent the degree of attacks and list the PSNR and NC (used to measure the similarity between two bi-level images) value of each attack in Fig. 3(e). Observing Table 3, we can see that our scheme is robust enough against some common attacks**.**



(a) (b) (c) (d) (e)

Figure 5. Proposed copyright protection scheme for color image (a) host image, (b) secret image, (c) master share, (d) ownership share and (c) stacked image

Table 3. Common Attacks

Attack	PSNR(dB)	NC (%)
Salt & Pepper	32.65	85.77
Gaussian noise	27.81	73.20
Image Cut	16.83	85.83
Sharpening	26.23	83.01
JPEG Compression	34.21	84.74
Image rotate	11.45	45.50

5. CONCLUSION

Undoubtedly, Visual Cryptography gives one of the protected approaches to exchange pictures on the Internet. The upside of visual cryptography is that it exploits human eyes to decode secret images with no computation required. In light of the hypothesis of color decomposition, every color on a color image can be deteriorated into three essential hues: C, M, and Y. With the halftone innovation, we can transform a color image into a half-toned image which is suitable for generating visual cryptography. As the traditional schemes for black-and-white visual cryptography, Young Chang Hou methods extend every pixel of a color secret image into a 2×2 block in the sharing images and keep two color and two transparent pixels in the block. Copyright assurance scheme for computerized color images utilizing Key based Visual Cryptography Watermarking was propose based on requirements of robustness and unambiguousness using visual cryptography and pseudorandom number generator. Moreover, the proposed scheme does not alter the host image, and can recognize the ownership without resorting to the original image. Hence, it is exceptionally reasonable to protect those digital images that cannot be altered, such as medical images. In proposed technique, it is completely used the benefits of VC, which can recuperate the secret image with human eyes without the guide of PCs. Security is likewise ensured by the two-out-of-two VC scheme, of which satisfied by pseudorandom number

generator. Consequently, without the right private key, no one can recover any meaningful image or acquire any secret information. Through the demonstration in section 4, we can see that our scheme is robust enough against some basic assaults. In the future, the issue of gray-level and color secret images will be further studied.

6. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[2] Naor, M., Shamir, A.: "Visual cryptography." In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995).

[3] Eisen PA, Stinson DR (2002) "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels", Des Codes Cryptograph 25:15–61.

[4] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.

[5] D.R. Stinson, "An Introduction to visual cryptography, presented at Public Key Solutions '97", Toronto, Canada, April 28–30, 1997.

[6] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," ACM Theor. Comput. Sci., vol. 250, pp. 143–161, 2001.

[7] V. Rijmen, B. Preneel, "Efficient color visual encryption for shared colors of Benetton," Eurocrypto'96, Rump Session, Berlin, 1996.

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

[9] Y.C. Hou, F. Lin, C.Y. Chang, "Improvement and implementation of the secret color image sharing technique", Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 592–597.

[10] Y.C. Hou, F. Lin, C.Y. Chang, "A new approach on 256 color secret image sharing technique", MIS Review, No. 9, December 1999, pp. 89–105.

[11] Y.C. Hou, C.Y. Chang, F. Lin, "Visual cryptography for color images based on color decomposition", Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 584–591.

[12] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography," in Proc. IEEE Int. Conf. Eng. Intell. Syst., 2006, pp. 1–5.

[13] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.

[14] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," Opt. Eng., vol. 44, p. 077003, 2005.

[15] M. Naor and B. Pinkas, "Visual authentication and identification," Adv. Cryptol., vol. 1294, pp. 322–336, 1997.

[16] W. Q. Y, J. Duo, and M. Kankanhalli, "Visual cryptography for print and scan applications," in Proc. IEEE Int. Symp. Circuits Syst., 2004, pp. 572–575.

[17] InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", in Proc. IEEE Tran. on Image Processing, Vol. 20, No. 1, January 2011, pp. 132-145.

[18] Ching-Sheng Hsu, and Young-Chang Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering 44(7), 077003 (July 2005), pp. 1-10.

[19] James E. Gentle, "Random Number Generation and Monte Carlo Methods", Springer (1998).

[20] J. A. Reeds, "Cracking a random number generator", Cryptologia, 1(1), 1977.