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

Review on Implementation of Random Grid Visual Cryptoraphy for Color Images

Snehal N. Meshram[1], Sneha U. Bohra[2]

[1]ME Scholar, Department of CSE, GHRCEM, Maharashtra, India

[2]Guide, Department of CSE, GHRCEM, Maharashtra, India

Abstract: ***Visual Cryptography is a special encryption technique that encrypts the secrect image into n numbers of shares to hide information in images in such a way that it can be decrypted by the human visual system. It is imperceptible to reveal the secret information unless a certain number of shares (K) or more are superimposed. Simple Visual Cryptography is very insecure. Variable length key based Visual Cryptography for color image uses a varible length Symmetric key based Visual Cryptography scheme for color images where a secrect key is used to encrypt the image and division of the encrypted image is done useing Random Number. Unless the secrect key is known, the original image will not be decrypted. Here secrect key ensures the security of images. The proposed method introduces the concept of above scheme.Encryption process encrypts Original Image using variable length Symmetric key, gives encrypted image. Share generation process divides the encrypted images into n number of shares using random number. Decryption process stacks k number of shares out of n to reconstruct encrypted image and uses the same key for decryption.***

Keyword: Visual Cryptography (VS), Random Numbers, Secret Sharing, Symmetric key

1. Introduction

Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers. Like other multimedia components, image sensed by human. Pixel is the smallest unit constructing a digital image.Each pixel of a 32 bit digital color image are divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. Human visual system acts as an OR function. Two transparent objects stacked together, produce transparent object. But changing any of them to non-transparent, final objects will be seen non-transparent. In k-n secret sharing visual cryptography scheme an image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the image. The division is done by Random Number generator. Visual Cryptography is a perfect way to provide the security for the confidential information. where binary pictures were considered in the encryption of pictures by two random grids. The encryption of a secret picture or shape into two random grids which are printed on transparencies such that the areas containing the secret information in the two grids are inter-correlated. Visual cryptography is basedon cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. Visual cryptography is a very secure and unique way to protect secrets.

Visual cryptography has two important features. The first feature is its perfect secrecy,and the second feature is its decryption method which requires neither complex decryption algorithms nor the aid of computers. Consider binary secret image B and a set of n participants sharing B. A k out of n visual secret sharing scheme encrypts B into n transparencies (called shares) which are distributed to the n participants one by one in such a way that only when k or more shares are stacked together can the participants see B by their visual system; while any group of less than k shares obtains nothing about B. The additive and subtractive color models 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.

2. Background

Visual Cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir. In a -out-of- 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 or more participants can visually reveal the secret image by superimposing any transparencies together. The secret cannot be decoded by any or fewer participants, even if infinite computational power is available to them. VC scheme proposed by Naor and Shamir 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, copyright protection, watermarking, visual authentication and identification, print and scan applications, etc.

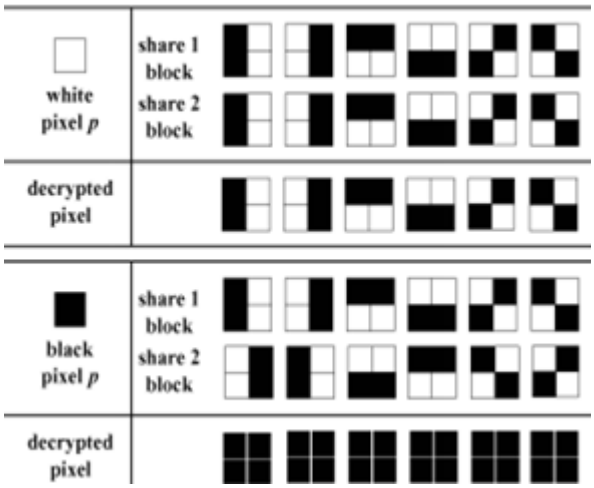

Figure 1: Construction of (2, 2) VC scheme: a secret pixel is encoded into four sub pixels in each of two shares. The decrypted pixel is obtained by superimposing the blocks in shares one and two.

Several new methods for VC have been introduced recently in the literature. Blundo proposed an optimal contrast k-out-of-n scheme to alleviate the contrast loss problem in there constructed images. Ateniese proposed a more general method for VC scheme based upon general access struc-ture. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The VC scheme concept has been extended to grayscale share images rather than binary image shares . Blundo proposed VC schemes with general access structures for grayscale share images. Hou transformed a gray-level image into halftone images and then applied binary VC schemes to generate grayscale shares. Al-though the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

Ateniese developed a method of extended visual cryptography (EVC) in which shares contain not only the secret information but are also meaningful images. Hypergraph colorings are used in constructing meaningful binary shares. Since hypergraph colorings are constructed by random distributed pixels, the resultant binary shares contain strong white noise eading to inadequate results. Wang generalized the Ate-niese's scheme using concatenation of basis matrices and the extended matrices collection to achieve more simpler deviation of basis matrices. Nakajima extended EVC to a scheme with natural grayscale images to improve the image quality.Zhou et al. used halftoning methods to produce good quality halftone shares in VC. Fu generated halftone shares hat carry visual information by using VC and watermarking methods. Myodo proposed a method to generate mean-ngful halftone images using threshold arrays. Wang et. al. produced halftone shares showing meaningful.

3. Related Work

In paper 1 has proposed, a serves as a basic model and has been applied to man applications. Aside from the obvious applications to information hiding, there are many applications of VC, which include general access structures, copyright protection ,watermarking, visual authentication and identification, print and scan applications. In paper 2 has introduced, a similar technique, called random grid encryption, in 1987. Roughly speaking, the model Proposed A secret image, known by a trusted party called the dealer, has to be shared among a set of participants in such a way that some subsets of participants, called qualified sets are able to visually recover the images while others, called forbidden sets, do not have any information about the secret image. In order to share the image, the dealer creates a share for each participant.In paper 3, 5 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 Elled withred, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identiEed from any one of these two shares alone. In paper 4, method has proposed a binary encoding to represent the subpixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking subpixels 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.In paper 12, 18 has proposed 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 diLcult to obtain totally random noise shares. Some image boundaries might be found on each share, thus compromising the secrecy required.In paper 20, 22 has proposed a VCS which has less pixel expansion than that in. In Yang proposed another one which achieves no pixel expansion. The scheme only supports black-and-white images. In 2007, Chen et al. extended the results to gray-scale images and proposed a gray-scale VCS with no pixel expansion. However, the scheme does not support the general *k*-out-of-*n* threshold setting. In addition, it also needs to perform block averaging (i.e. preprocessing) on the original image before carrying out the secret sharing. Another gray-scale VCS without pixel expansion was proposed by Chan et. in 2004. The scheme also needs preprocessing by dithering and adjusting the gray level of the original image. The general *k*-out-of-*n* threshold setting is not supported either.In paper Hou proposed another color VC scheme. Based on the halftone technique and color decomposition, it decomposes the secret image into three colors *C*, *M* and *Y*. By manipulating the three color values, the color pixels in the secret image can be represented. However, similar to what happens in the shares are meaningless. The shares such schemes as those generated in are meaningless and look like random dots. With such appearance, they make easy targets for attackers to zero in; whether or not the secrets can be easily cracked open, the looks of the meaningless shares are already revealing the existence of secrets to attackers. In paper 7, 9

has introduced Key Lab.Of Inf. Security, Chinese Acad. Of Sci., Beijing, China Chuankun Wu Xijun Lin explains construction of visual cryptography schemes in detail. The size of generated transparencies is unexpanded. Storing the shares in a safe repository. Enhancing the visual clarity of the image before processing the images. Visual cryptography provides a secure way to secure images. In this paper, the author discussed about the cheating problem in VC and extended VC. They've considered the attacks of malicious adversaries who may deviate from the scheme in any way. This paper has proposed three cheating methods and applied them on attacking existent VC or extended VC schemes. Visual cryptography scheme encodes a black & white secret image into n shadow images called shares which are distributed to the n participants.In paper 31,32 has developed the Visual Secret Sharing Scheme(VSSS) to implement this model[Naor95]. In *k* out of *n* VSSS(which is also called (*k*, *n*) scheme), an binary image(picture or text) is transformed into *n* sheets of transparencies of random images. The original image becomes visible when any *k* sheets of the *n* transparencies are put together, but any combination of less than *k* sheets cannot reveal the original binary image. In the scheme, one pixel of the original image is reproduced by *m* subpixels on the sheets. The pixel is considered "on"(transparent) if the number of transparent subpixels is more than a constant threshold, and "off" if the transparent subpixels is less than a constant lower threshhold. when the sheets are stacked together. The contrast α is the difference between the on and off thresh hold number of transparent pixels

4. Conclusion

In the above literatre survey we have proposed a technique of well known k-n secret sharing on color images using a variable length key with share division using random number. As we know Decryption part of visual cryptography is based on OR operation, so if a person gets sufficient k number of shares; the image can be easily decrypted. Key adds robustness to the visual cryptography techniques and variable length of the key makes it more secure. At the time of dividing an image into n number of shares we have used random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images This technique only checks „1 at the bit position and divide that „1 into (n-k+1) shares using random numbers. A comparison is made with the proposed scheme with some other schemes to prove the novelty of the scheme.

References

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT , 1994, pp. 1–12.
[2] 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.
[3] 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.
[4] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int.Conf. Multimedia Expo, 2004, pp. 975–978.
[5] 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.
[6] M. Naor and B. Pinkas, "Visual authentication and identification," Adv. Cryptol., vol. 1294, pp. 322–336, 1997.
[7] 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.
[8] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, 1987.
[9] V. Rijmen, B. Preneel, ELcient colour visual encryption for shared colors of Benetton, Eurocrypto'96, Rump Session, Berlin, 1996.
[10] 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.
[11] 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.
[12] 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, November1999, pp. 584–591.
[13] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, vol. 25, no. 4, pp. 481–494, March 2004.
[14] Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, and Y. P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," Information Sciences, vol. 177, no. 21, pp. 4696–4710, November 2007.
[15] 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, no. 1, 2004.
[16] Y. C. Hou, "Visual cryptography for color images," Pattern Recognition, Vol. 36, pp.1619-1629, 2003.
[17] C. N. Yang and C. S. Laih, "New colored visual secret sharing schemes," Designs, Codes and Cryptography, Vol. 20, No. 3, pp. 325-335, 2000.
[18] Naor95 M. Naor and A. Shamir. Visual cryptography, advances in cryptology. Eurocrypt'94 Proceeding LNCS, 950:1–12, 1995.
[19] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1-12.
[20] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryp-tography for general access structures," Inf. Comput., vol. 129, no. 2,pp. 86–106, 1996.
[21] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking,"in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.
[22] M. Naor and B. Pinkas, "Visual authentication and identification," Adv.Cryptol., vol. 1294, pp. 322–336, 1997.

[23] W. Q. Y, J. Duo, and M. Kankanhalli, "Visual cryptography for printand scan applications," in Proc. IEEE Int. Symp. Circuits Syst., 2004,pp. 572–575.
[24] C. Blundo, P. D'Arco, A. D. S. , and D. R. Stinson, "Contrast optimalthreshold visual cryptography schemes," SIAM J. Discrete Math., vol.16, no. 2, pp. 224–261, 2003.[9] L. A. MacPherson, "Gray level visual cryptography for general accessstructrue," M. Eng. thesis, [1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT , 1994, pp. 1–12.
[25] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryp- tography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.
[26] 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.
[27] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.
[28] 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.
[29] M. Naor and B. Pinkas, "Visual authentication and identification," Adv. Cryptol., vol. 1294, pp. 322–336, 1997.
[30] 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.
[31] C. Blundo, P. D'Arco, A. D. S. , and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.
[32] L. A. MacPherson, "Gray level visual cryptography for general access structrue," M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000. Univ. Waterloo, Ontario, Canada, 2000.