Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Visual Cryptography to Secure Biometric Database: A Review

Sonal Wange

Department Of Information Technology,
KGIET, Darapur, India

Abstract— Over the past few years, there is increasing concern over personal information in computer systems has increased interest in data security like Visual Cryptography. Visual cryptography divides secret images into one and more random shares and provides secured digital transmission which is used only for one time. The original images can be reuse by using this scheme. It is easy and uncomplicated technique to execute the secret image for shadow images (share of image). In this paper concept of visual cryptography is discussed which is a perfectly secure method of keeping images secret, for feasible use in biometric identification technique and protection such as fingerprint images for the purpose of user authentication along with various visual cryptography schemes as an literature review. This paper not only reviews how to apply sharing of single secrete image and multiple secrete image on black and white as well as on color images but also a comparative analysis on various visual cryptography schemes is also performed .

Keywords— Visual Cryptography, Single Secrete Image, Multiple Secrete Image, Shadow Images, Biometric Identification.

I. INTRODUCTION

Visual cryptography is the art of encrypting information such as handwritten text, images etc. in such a way that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. A secret image consists of a collection of black and white pixels. Here each pixel is treated independently. For encoding the secret image, we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivided into n black and white sub-pixels. For decoding the image, a subset S of those n shares are picked and copied on separate transparencies [1]. Visual cryptography schemes were independently introduced by Shamir. Shamir divided data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of k – 1 pieces reveals absolutely no information about D. This technique allow the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces [2].

The first form of visual cryptography is also known as secret sharing. The simplest form of visual cryptography separates a secret image into two parts so that either part by itself conveys no information. When these two parts are combined together by means of superimposition, the original secret can be revealed. These parts are called as shares. There are several advantages of visual cryptography. Basically it is simple to use and no mathematical computations are required to reveal the secret. Secondly, the individuals who do not have knowledge of cryptography are indirectly getting involved in decryption. The major drawback found in this scheme is that visually blind people cannot make use of this technique as we perform the encryption by making the share and person who perform the encryption those people only able to find the exact shares for performing the decryption. The example of visual cryptography is shown in Fig.1 [5].The first two part represent the shares and third part of fig shows decoded password.

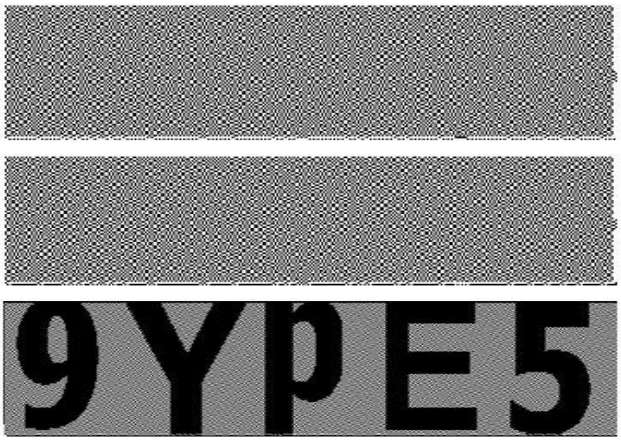

Fig. 1 An example of visual cryptography.

II. LITERATURE REVIEW

A. Black And White Visual Cryptography Scheme :

The visual cryptography scheme is used for encrypting the information. Visual cryptography is a one of the technique of encryption which is used to hide the information in an image; decryption can be done by human visual system. By using only this type of cryptography, no one is able reuse the data. The image which we can recover after decryption will not be same as original image so it cannot be reused. There are number of visual cryptography schemes in existence. Some of them are described below.

1) *Sharing Single Secret Image :* In this type of visual cryptography scheme, the secret image is divided into exactly two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with remote voting system that uses 2 out of 2 secret sharing schemes for authentication purpose. To reveal the original image, these two shares are required to be stacked together [20], [21]. Naor and Shamir's [13] proposed encoding scheme to share a binary image into two shares. i.e. Share1 and Share2. If pixel is white one of the above two rows of table from fig 2.1 is chosen to generate Share1 and Share2 , likewise If pixel is black one of the below two rows table of fig 2.1 is chosen to generate Share1 and Share2. Here each share of pixel p is encoded into two white and two black pixels. Each share alone gives no hint about the pixel p. That is share is not provide any information whether it is white or black. Secret image is shown only when both shares of images are overlaid or superimposed.

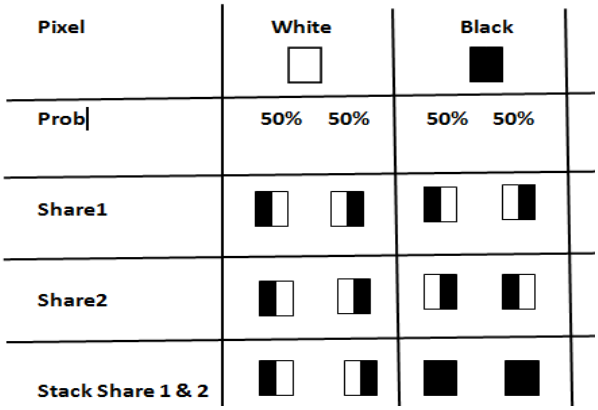

Fig. 2 Basic concept of 2 out of 2 scheme

2) Sharing Multiple Secret Images: Wu and Chen [14] were first researchers to present the visual cryptography schemes to share two secret images in two shares. He hidden two secret binary images into two random shares, that is A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by first rotating A Θ anti-clockwise. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180◦ or 270◦. To overcome the angle restriction of Wu and Chen's scheme [14].Wu and Chang [36] also refined the idea of Wu and Chen [14] by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90◦, 180◦ or 270◦) can be removed.

S J Shyu [37] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of n≥2 secrets into two circle shares. In this the n secret image can be obtained one by one by loading the first share and the rotated second shares with n different rotation angles. For encoding purpose unlimited shapes of image and to remove the limitation of transparencies to be circular, Fang [4] offered reversible visual cryptography scheme. In this scheme two secret images which are encoded into two shares; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them. Jen-Bang Feng [38] developed a visual secret sharing scheme for hiding multiple secret images into two shares. This scheme analyzes the secret pixels and the corresponding share blocks to construct a stacking relationship graph. In this the vertices denote the share blocks and the edges denote two blocks stacked together at the desired decryption angle. By using this graph and the pre-defined visual pattern set, two shares are generated. To provide more randomness for generating the shares Mustafa Ulutas [39] advised secret sharing scheme based on the rotation of shares. In this scheme shares are of rectangular shape and they are created in a fully random manner. Stacking of the two shares reconstructs the first secret. Rotating the first share by 90° counterclockwise and stacking it with the second share reconstructs the second secret. Tzung-Her Chen [40] proposed the multiple image encryption schemes by rotating random grids, without using any pixel expansion and codebook redesign. To encode four secrets into two shares and recovering the reconstructed images without distortions Zhengxin Fu [41] intended a rotation visual cryptography scheme. Rotational visual cryptography scheme construction was based on correlative matrices set and random permutation, which can be used to encode four secret images into two shares. Jonathan Weir [42] suggested sharing multiple secrets using visual cryptography. A master key is generated for all the secret images; correspondingly, secret images are shared using the master key and multiple shares are obtained. This kind of scheme allows dividing a secret into K number of shares. Then the secret can be open from any N number of Shares among K. The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption. The application of this scheme is usually found with banking system. In the joint accounts, three shares are

created. One is reserved with bank's server, second is given to the one customer for the joint account and third share is delivered to the second customer. Hence both customers are able to access the account [22].

All the above schemes can be used only to share the black and white secret images, but it is need of time that schemes should also support color images. To meet this demand we are going to review on the shares of the color images.

B. Color Visual Cryptography Schemes :

I. Sharing Single Secret Image:

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [7]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In the c-colorful visual cryptography scheme one pixel is transformed into the m sub pixels, and each sub pixel is divided into the c color regions. In each and every sub pixel, there is exactly one color region is colored, and all the other color regions are black. The color of one pixel depends on the inter relationships between the stack sub pixels. In this colored visual cryptography scheme with c colors, the pixel expansion m is c× 3. Yang and Laih [8] improved the pixel expansion to c × 2 of Verheul and Van Tilborg [7]. But in both of these schemes share generated were meaningless.

For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai [9] anticipated color visual cryptography scheme. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then as per predefined Color Index Table, the secret color image will be hidden into two conceal images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table. In this scheme also number of sub pixels is in proportional to the number of colors in the secret image as in Verheul and Van Tilborg [7] Yang and Laih [8] schemes. When more colors are there in the secret image the larger the size of shares will become. To overcome this limitation Chin- Chen Chang [10] developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more professional way to hide a gray image in different shares. In this scheme of cryptography size of the shares is fixed; it does not vary when the number of colors showing in the secret image differs. This scheme does not require any predefined Color Index Table. Though pixel expansion is a fixed in [10] this scheme is not suitable for true- color secret image. For sharing true-color image Lukac and Plataniotis [11] introduced bit-level based scheme by operating directly on S-bit planes of a secret image. To hide a color secret image into multiple colored images it is desired that the generated camouflage images contain less noise. For this purpose R.Youmaran [12] invented an improved visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. For reducing pixel expansion in color visual cryptography scheme S.J.Shyu [33] advised a more efficient colored Visual secret sharing scheme with pixel expansion of |log2c*m| where m is the pixel expansion of the exploited binary scheme. By allowing for color image transmission over bandwidth constraint channels a cost effective visual cryptography scheme was invented by Mohsen Heidarinejad [34]. The solution offers perfect reconstruction while producing shares with size smaller than that of the input image using maximum distance separable. This scheme provides pixel expansion which is less than one. To get better speed of encoding Haibo Zhang [35] presented a multi-pixel encoding which can encode variable number of pixels for each run. F. Liu [16] developed a color visual cryptography scheme under the visual cryptography model of Naor and Shamir with no pixel expansion. In this scheme increasing the number of colors of recovered secret image does not increases pixel expansion. Wei Qiao [17] suggested visual cryptography scheme for color images based on halftone technique. A secret image sharing scheme for true-color secret images devised by Du-Shiau Tsai [18]. In the proposed scheme through combination of neural networks and variant visual secret sharing, In this technique the quality of the reconstructed secret image and hide images are visually the same as the corresponding original images. For encoding multiple color images using visual cryptography little researches have been carried out that are discussed here.

II. *Sharing Multiple Secret Images:*

Tzung-Her Chen [40] anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The policy of traditional visual secret image sharing implemented to generate share images macro block by macro block in such a way that multiple copies secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for binary, gray and color secret images with pixel expansion of 4. Daoshun Wang [19] provided general construction for extended visual cryptography schemes using matrix extension algorithm. A simple construction method for single or multiple and binary, gray scale, color secret images using matrix extension utilizing meaningful shares with of suggested. Using matrix extension algorithm, any existing visual cryptography scheme with random-looking shares can be easily modified to utilize meaningful shares.

III. COMPARATIVE STUDY OF VARIOUS VISUAL CRYPTOGRAPHY SCHEME

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [13] suggested two main parameters: pixel expansion m and contrast α.

Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It shows the loss in resolution from the original picture to the shared one. Contrast α is the

difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Jung-San Lee [43] suggested security, pixel expansion, accuracy and computational complexity as a performance measures. Security is fulfilled if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected. Accuracy is measured to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR) measure. The computational complexity is concerns with the total number of operators required both to generate the set of n shares and to restructure the original secret image C.

Chang [9] suggested that visual cryptography scheme should support wide image format like color and gray scale. Author also argued that the random looking shares appear to be suspicious and thus are vulnerable to attacks by attackers in the middle, to fill up this security gap, meaningful shares should be produced. Jen-Bang Feng [38] suggested that VCS should support multiple secret to work efficiently. If the scheme support only one secret to share at a time to share multiple secret images numerous share have to be produced, transmitted and maintained.

Comparative study of different single share and multi share visual cryptography scheme is given by table I and II respectively.

The list of Abbreviations used in Visual Cryptography Schemes:
m indicate pixel expansion of corresponding visual cryptography schemes,
c indicate number of colors in visual cryptography schemes,
n indicate the number of shares.

A. Sharing Single Secret Image:

TABLE I
COMPARATIVE STUDY OF SHARING SINGLE SECRET IMAGES VCS.

Sr. No.	Author	Year	Pixel Exapansion	Image Format	Type Of Image generated
1	Naor and Shamir[13]	1995	4	Binary	Random
2	Chin-Chen Chang[10]	2005	4	Binary	Meaningful
3	Liguo Fang[39]	2006	2	Binary	Random
4	Xiao-qing Ta[38]	2009	1	Binary	Random
5	E. Verheuland[7]	1997	C^*3	color	Random
6	C.Yang and C. Laih[8]	2000	C^*2	color	Random
7	C.Chang, C. Tsai[9]	2000	529	color	Random
8	Chin-Chen Chang[10]	2002	9	Gray	Meaningful
9	L. R. Lukac[11]	2005	2	color	Random
10	R.Youmaran[12]	2006	9	color	Meaningful
11	S.J. Shyu[33]	2006	$[\log_2 C^* m]$	color	Random
12	Mohsen Heidarinejad[34]	2008	916	color	Random
13	Haibo Zhang[35]	2008	1	Gray	Random
14	F. Liu[16]	2008	1	color	Random
15	Wei Qiao[17]	2009	M	color	Random
16	Du-Shiau Tsai[18]	2009	9	color	Meaningful

B. Sharing Multiple Secret Images:

TABLE III: COMPARATIVE STUDY OF SHARING MULTIPLE SECRET IMAGES VCS.

Sr. No.	Author	Year	No. Of Secrete Image	Pixel Exapansion	Image Format	Type Of Image generated
1	Wu and Chen[14]	1998	2	4	Binary	Random
2	H.-C.Hsu[15]	2004	2	4	Binary	Random
3	Wu and Chang[36]	2005	2	4	Binary	Random
4	S.J.Shyu[37]	2007	n(n>=2)	2n	Binary	Random
5	W.P. Fang[4]	2007	2	9	Binary	Random
6	Jen-Bamb Feng[3]	2008	n(n>=2)	3n	Binary	Random
7	Mustafa Ulutas[6]	2008	2	4	Binary	Random
8	Tzung-Her Chen[40]	2008	2	1	Binary	Random
9	Tzung-Her Chen[18]	2008	n(n>=2)	4	Binary,	Random
10	Zhengxin Fu[41]	2009	4	9	Binary	Random
11	Jonathan Weir[42]	2009	n	4	Binary, gray, Color	Random

IV. VISUAL CRYPTOGRAPHY IN BIOMETRIC APPLICATIONS

Visual Cryptography is very useful to secure a biometric (science of establishing the identity of an individual based on physical or behavioral traits such as face, fingerprints, iris, gait, and voice) [23]database template.A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., face image), extracting a feature set from the data (e.g., Eigen-coefficients), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify for a claimed identity. The template of a person in the database is generated during enrollment and is often stored along with the original raw data. This has heightened the need to accord privacy to the subject by adequately protecting the contents of the database. For securing the privacy of an individual enrolled in a biometric database, Davida. [24] and Ratha. [25] proposed storing a transformed biometric template instead of the original biometric template in the database. This was referred as a private template [24] or a cancelable biometric [25]. Newton. [28] and Gross. [29] introduced a face de-identification algorithm that minimized the chances of performing automatic face recognition while preserving details of the face such as expression, gender, and age. Bitouk [30] proposed a face swapping technique which protected the identity of a face image by automatically substituting it with replacements taken from a large library of public face images. However, in the case of face swapping and aggressive de-identification, the original face image can be lost. Recently, Moskovich and Osadchy [31] proposed a method to perform secure face identification by representing a private face image with indexed facial components extracted from a public face database. Figs. 3.1 and 3.2 show block diagrams of the three biometric modalities. During the enrollment process, the private biometric data is sent to a trusted third-party entity. Once the trusted party receive it, the biometric data is decomposed into two images(shares) and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. During the authentication process, the trusted party sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in steganography [28],or cryptosystem [32] approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image.

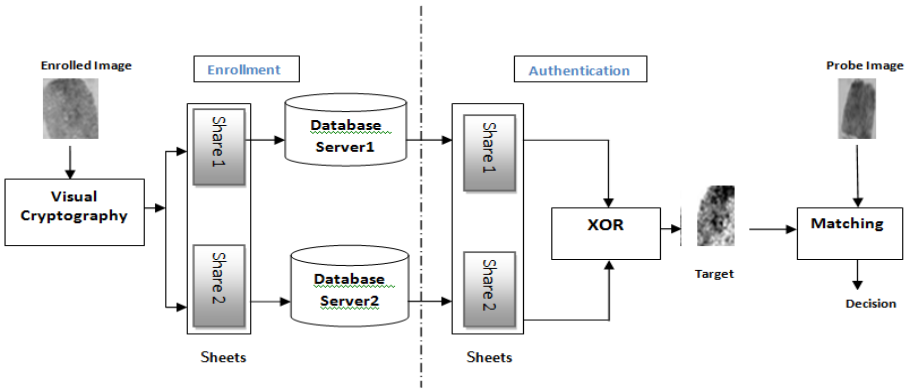

Fig. 3 System for de-identifying and storing a fingerprint image. A similar technique is used for iris codes.

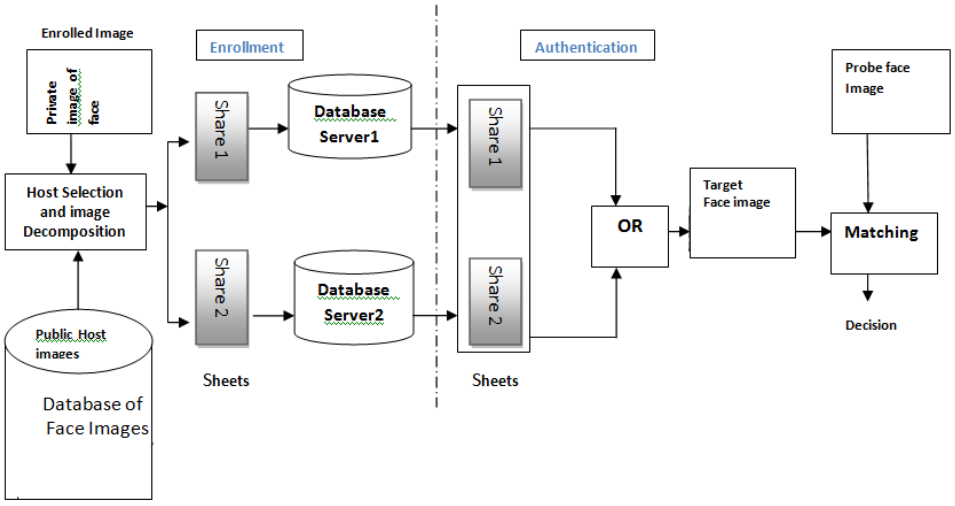

Fig. 4 System for de-identifying and storing a face image.

V. ADVANTAGES

Among the various advantages of Visual Cryptography Schemes one of the advantage of VCS is that it performs decoding relies purely on human visual system, which leads to a lot of interesting applications in private and public sectors of our society.

VI. DISADVANTAGES

Visual Cryptography is used with short messages, therefore it gives the cryptanalyst little to work with. As with any type of analysis techniques, it having little cipher text inhibits the effectiveness of a technique being used to break an encryption Since Visual Cryptography uses very short message, public keys can be encrypted using this method. Visual Cryptography technique has proved that security can be attained with even simple encryption schemes.

VII. CONCLUSION

This survey is very useful to understand different scheme of visual cryptography techniques implement in the biometric applications and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. While selecting any visual cryptography technique for a particular application Table 3.1 and 3.2 is helpful. The comparative study of different visual cryptography techniques helps us to find better method to provide security to our biometric database template.

REFERENCES

[1] Hegde C ,Manu S, Shenoy P D, Venugopal, K. R., Patnaik L. "*Secured Authentication using Image Processing and Visual Cryptography for Banking Applications*," in Proceedings of 16 Th IEEE International Conference on Advanced Computing and Communications, ADCOM 2008,2008, pp. 65-72.

[2] Adi Shamir, "*How to Share a Secret," in* Communications of ACM, Vol. 22, no.11, 1979, pp. 612-613.

[3] Jen-Bang Feng, Hsien-ChuWu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, "*Visual Secret Sharing For Multiple Secrets*", Pattern Recognition 41, pp.3572–3581, 2008.

[4] Wen-Pinn Fang, "*Visual Cryptography In Reversible Style*", IEEE Proceedingon the Third International Conference on ntelligent Information Hidingand Multimedia Signal Processing (IIHMSP2007, Kaohsiung, Taiwan, R.O.C,2007.

[5] Pallavi V. Chavan, R.S. Mangrulkar, "*Sharing a Secret inNetwork*," in International Engineering and Technology Journalof Information System, Vol.4, no. 2, pp.83-87.

[6] Mustafa Ulutas, Rıfat Yazıcı, Vasif V.Nabiyev, Güzin Ulutas, (2,2)- "*Secret Sharing Scheme With Improved Share Randomness*",978-1-4244-2881- 6/08,IEEE,2008.

[7] E. Verheuland H. V. Tilborg, "Constructions *And Properties Of K Out Of N Visual Secret Sharing Schemes. "*Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.

[8] C.Yang and C. Laih, *"New Colored Visual Secret Sharing Schemes*". Designs, Codes and cryptography, 20, pp. 325–335, 2000.

[9] 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, pp. 21–27,July 2000.

[10] Chin-Chen Chang, Tai-Xing Yu, "*Sharing A Secret Gray Image In Multiple Images*", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[11] R. Lukac, K.N. Plataniotis, "Bit-*Level Based Secret Sharing For Image Encryption*", Pattern Recognition 38 (5), pp. 767–772, 2005.

[12] R.Youmaran, A. Adler, A.Miri, "*An Improved Visual Cryptography Scheme For Secret Hiding*", 23rd Biennial Symposium on Communications, pp. 340-343, 2006. Acquisition and Modeling, pp. 340-344, 2008.

[13] Moni Naor and Adi Shamir, "*Visual Cryptography*", advances incryptology–Eurocrypt, pp1-12,1995.

[14] C.C. Wu, L.H. Chen, "*A Study On Visual Cryptography*", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[15] H.-C.Hsu, T.-S. Chen,Y.-H.Lin, "*The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing*", in Proceedings of the 2004 IEEE International Conferenceon Networking, Sensing & Control, Taipei, Taiwan, pp.996–1001, March2004.

[16] F. Liu1, C.K. Wu X.J. Lin, "*Colour Visual Cryptography Schemes*", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.

[17] Wei Qiao, Hongdong Yin, Huaqing Liang, "*A kind Of Visual Cryptography Scheme For Color Images Based On Halft one Technique*", International Conference on Measuring Technology and Mechatronics Automation 978-0-7695-3583-8/09, pp. 393-395, 2009.

[18] Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-TeHuang, "A Novel *Secret Image Sharing Scheme For True-Color Images With Size Constraint*", Information Sciences 179 3247–3254 Elsevier, 2009.

[19] Daoshun Wang, Feng Yi, XiaoboLi, "*On General Construction For Extended Visual Cryptography Schemes*", Pattern Recognition 42(2009), pp 3071– 3082, 2009

[20] Zhongnin Wangarce, G.R., "*Halftone Visual Cryptography by Interative Halftoning*," *in Proceedings of 2010 IEEEInternational Conference on Acoustics Speech and Signal Processing (ICASSP)*, March 2010, pp. 1822-1825.

[21] Tzung, Chang Sain, Wei Lee, "*A Novel Subliminal Channel Found in Visual Cryptography and Its Application to Image Hiding*", in *Proceedings of* 3rd *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Vol. 1, 2007,pp. 421-424.

[22] Che Lee, Wen Tsai, " *Authentication of Binary Images in PNG Format Based on a Secret Sharing Technique*," in *Proceedings of IEEE International Conference on System and Engineering*, *Taipei*, July 2010, pp. 506-510.

[23] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York:Springer, 2007.

[24] G. I. Davida, Y. Frankel, and B. J. Matt, "*On enabling secure appli-cations through off-line biometric identification*," inProc. IEEE Symp.Security and Privacy, 1998, pp. 148–157.

[25] N. Ratha, J. Connell, and R. Bolle, "*Enhancing security and privacy in biometrics-based authentication systems,"*IBM Syst. J., vol. 40, no. 3,pp. 614–634, 2001.

[26] Y. Feng, P. Yuen, and A. Jain, "*A hybrid approach for face template protection*" ,inProc. SPIE Conf. Biometric Technology for Human Identification, Orlando, FL, 2008, vol. 6944.

[27] N. Agrawal and M. Savvides, "*Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching*", inProc. Computer Visionand Pattern Recognition Workshop, 2009, vol. 0, pp. 85–92.

[28] E. M. Newton, L. Sweeney, and B. Malin, "*Preserving privacy by de-identifying face images*,"IEEE Trans. Knowl. Data Eng., vol. 17,no. 2, pp. 232–243, Feb. 2005.

[29] R. Gross, L. Sweeney, F. De la Torre, and S. Baker, "*Model-based face de-identification*," inIEEE Workshop on Privacy Research in Vision, Los Alamitos, CA, 2006.

[30] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "*Face swapping: Automatically replacing faces in photographs*,"ACM Trans.Graph., vol. 27, no. 3, pp. 1–8, 2008.

[31] B. Moskovich and M. Osadchy, "*Illumination invariant representation for privacy preserving face identification*," in Proc. IEEE ComputerSociety and IEEE Biometrics Council Workshop on Biometrics, San Francisco, CA, Jun. 2010, pp. 154–161.

[32] A. Jain, K. Nandakumar, and A. Nagar, "*Biometric template security*," EURASIP J. Advances Signal Process., pp. 1–17, 2008.1. M. Naor and A. Shamir, Visual cryptography, in "Advances in Cryptology { EUROCRYPT '94", A.De Santis, ed., Lecture Notes in Computer Science 950 (1995), 1-12.

[33] S.J. Shyu, "*Efficient Visual Secret Sharing Scheme For Color Images*", Pattern Recognition 39(5) ,pp. 866–880, 2006.

[34] Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantinos N, Plataniotis "*Algebraic Visual Cryptography Scheme For ColorImages*", ICASSP, pp. 1761-1764, 2008.

[35] Haibo Zhang,Xiaofei Wang,WanhuaCao,YoupengHuang, "*Visual Cryptography For General Access Structure By Multi- Pixel Encoding With Variable Block Size*", International Symposium on Knowledge

[36] H.-C. Wu, C.-C. Chang, "*Sharing Visual Multi-Secrets Using Circle Shares*", Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).

[37] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, andK. Chen, "*Sharing multiple secrets in visual cryptography*", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007

[38] Xiao-qing Tan, "*Two Kinds Of Ideal Contrast Visual Cryptography Schemes*", International Conference on Signal Processing Systems, pp. 450-453, 2009. 2005.

[39] Liguo Fang, BinYu, "*Research On Pixel Expansion Of (2,n) Visual Threshold Scheme*", 1st International Symposium on Pervasive Computing and Applications ,pp. 856-860, IEEE.

[40] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "*Multiple-Image Encryption By Rotating Random Grids*", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[41] Zhengxin Fu, Bin Yu, "*Research On Rotation Visual Cryptography Scheme*", International Symposium on Information Engineering and Electronic Commerce, pp533-536, 2009.

[42] Jonathan Weir, WeiQi Yan, "*Sharing Multiple SecretsUsing Visual Cryptography*", 978-1-4244-3828-0/09, IEEE, pp 509-512, 2009.

[43] Jung-San Lee, T. Hoang Ngan Le, "*Hybrid (2, N) Visual Secret Sharing Scheme For Color Images*", 978-1-4244-4568-4/09, IEEE, 2009.

