International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.5, May 2012 – www.ijais.org

A Novel Face Template Protection Scheme based on Chaos and Visual Cryptography

Divya James
Department of Computer Science, Rajagiri School of Engineering and Technology, Kochi, India

Mintu Philip
Department of Computer Science, Rajagiri School of Engineering and Technology, Kochi, India

ABSTRACT
Protection of biometric data and templates is a crucial issue for the security of biometric systems This paper proposes new security architecture for protection of face templates using visual cryptography and chaotic image encryption. The use of visual cryptography is explored to preserve the privacy of biometric image by decomposing each private face image into two independent public host images such that the original image can be revealed only when both images are simultaneously available. The algorithm ensures protection as well as privacy for image using a fast encryption algorithm based on chaotic encryption. Chaos based cryptography is applied on to individual shares. Using this one can cross verify his identity along with the protection and privacy of the image.

Keywords
visual cryptography, security, chaotic, Arnold map

1. INTRODUCTION
Biometric based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards (ID), passwords, etc. One of the main reasons for this popularity is the ability of the biometrics technology to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person [1]. Among various commercially available biometric techniques such as face, voice, fingerprint, iris, etc., fingerprint-based and face recognition techniques are the most extensively studied and the most frequently deployed. While biometric techniques have inherent advantages over traditional personal identification techniques, the problem of ensuring the security and integrity of the biometric data is critical.

Researchers have proposed conventional algorithms such as AES, DES for the protection of biometric templates. However all the conventional algorithms take high processing power and high encryption/decryption time. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms.

So we introduce a new method for ensuring the security and integrity of biometric data which utilizes both visual cryptography and chaos-based cryptographic scheme. The model is achieved by using visual cryptography for obtaining shares of biometric images. Chaos based system is used for encryption. This algorithm encrypts image shares pixel by pixel taking consideration the values of previously encrypted pixels.

This paper is organized as follows: Section 2 deals with the related work and Section 3 and 4 deals with visual cryptography and 3Dchaotic map. Section 5 presents the proposed system and Section 6 deals with results and analysis. Section 7 contains the conclusion.

2. RELATED WORK

2.1 Visual Cryptography
One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir [2] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. Visual cryptography schemes were independently introduced by Shamir [3] and Blakely [4], their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols [5] and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles. A segment-based visual cryptography suggested by Borchert [6] can be used only to encrypt the messages containing symbols, especially numbers like bank account number, amount etc. The VCS proposed by Wei-Qi Yan et al., [7] can be applied only for printed text or image. A recursive VC method proposed by Monoth et al., [8] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. Similarly a technique proposed by Kim et al., [9] also suffers from computational complexity, though it avoids dithering of the pixels. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [10],[11],[12]. In these cases all participants who hold shares are assumed to be honest, that is, they will not present false or fake shares during the phase of recovering the secret image. Thus, the image shown on the stacking of shares is considered

as the real secrete image. But, this may not be true always. So cheating prevention methodologies are introduced by Yan et al., [13], Horng et al., [14] and Hu et al., [15]. But, it is observed in all these methodologies, there is no facility of authentication testing.

2.2 Chaos based Cryptography

In recent years, chaotic maps have been employed for image encryption. Most chaotic image encryptions (or encryption systems) use the permutation-substitution architecture. These two processes are repeated for several rounds, to obtain the final encrypted image. For example Fridrich suggested a chaotic image encryption method composed of permutation and substitution [16]. All the pixels are moved using a 2D chaotic map. The new pixels moved to the current position are taken as a permutation of the original pixels. In the substitution process, the pixel values are altered sequentially. Chen et al. employed a three-dimensional (3D) Arnold cat map[17] and a 3D Baker map in the permutation stage[18]. Guan et al. used a 2D cat map for pixel position permutation and the discretized Chen's chaotic system for pixel value masking[19]. Lian et al. used a chaotic standard map in the permutation stage and a quantized logistic map in the substitution stage[20]. The parameters of these two chaotic maps are determined by a key stream generated in each round. Gao et al. present the image encryption algorithm based on a new nonlinear chaotic algorithm using a power function and a tangent function instead of a linear function. It also uses a chaotic sequence generated by a nonlinear chaotic algorithm to encrypt image data using XOR operation[21].

3. VISUAL CRYPTOGRAPHY

VCS allows one to encode a secret image into sheet images, each revealing no information about the original. Since these sheets appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern, the sheets could be reformulated as natural images as stated by Naor and Shamir [22]. Ateniese et al. [24] introduced such a framework known as the extended VCS. Nakajima and Yamaguchi [23] proposed a theoretical framework to apply extended visual cryptography on grayscale images (GEVCS) and also introduced a method to enhance the contrast of the target images. The GEVCS operates by changing the dynamic range of the original and host images, transforming the gray-level images into meaningful binary images (also known as halftoned images) and then applying a Boolean operation on the halftoned pixels of the two hosts and the original image. However, some of these pixels (in the host and the original) have to be further modified. This is explained in more detail below.

3.1 Digital Halftoning and Pixel Expansion

Digital halftoning is a technique for transforming a digital gray-scale image to an array of binary values represented as dots in the printing process [25]. Error diffusion is a type of halftoning technique in which the quantization error of a pixel is distributed to neighboring pixels which have not yet been processed. Floyd and Steinberg [26] described a system for performing error diffusion on digital images based on a simple kernel. Their algorithm could also be used to produce output images with more than two levels. So, rather than using a single threshold to produce a binary output, the closest permitted level is determined and the error, if any, is diffused to the neighboring pixels according to the chosen kernel. Therefore, grayscale images are quantized to a number of levels equaling the number of subpixels per share. During the dithering process at the pixel level[27], any continuous tone pixel is expanded to a matrix of black and white subpixels defined by the gray level of the original pixel. The proportion of white subpixels in this matrix is referred to as pixel transparency. In our application, the host images used for encrypting a private face image and the private image itself are converted to halftoned images.

3.2 Encryption

The encryption process is applied on a pixel-by-pixel basis using the three halftoned images [27] (the two hosts and the original image). The arrangement of the subpixels in the shares of both the hosts has to be controlled such that the required transparency (the number of white subpixels) of the target pixel is obtained. The arrangement is determined based on the pixel transparencies triplet (t_1, t_2, t_T). t_1, t_2, and t_T are transparencies of the entire subpixel region for share 1, share 2, and the target, respectively.

The security of the scheme is also important. Therefore, during encryption, a Boolean matrix is randomly selected from a set of $2 \times m$ Boolean matrices $C t_T^{t_1, t_2}$ for every pixel in the original image. This is the primary difference between this scheme and Naor-Shamir's scheme: in the latter, only a single collection of matrices is required which depends on the number of hosts and the pixel expansion. Nakajima and Yamaguchi describe in detail the method to compute this collection of Boolean matrices [23].

However there are cases when the required transparency for the corresponding pixel in the target image cannot be obtained, no matter how the shared subpixels are rearranged. Therefore, to determine if it is possible to obtain the target transparency by rearranging the transparent (white) subpixels in the shares, the target transparency must be within the following range [condition (T1)] [23]:

$$t_T \in [\max(0, (t_1 + t_2 - 1)), \min(t_1, t_2)]$$

where t_1, t_2 and t_T ($\in [0,1]$) are the transparencies of the entire pixel region for share 1, share 2, and the target, respectively. The range of each of these transparencies for the entire image corresponds to the dynamic range of the pixel intensities of the respective images. The encryption process[23] consists of determining the arrangements of transparent subpixels on each sheet according to the pixel transparencies t_1, t_2 and t_T [27]. Here, one pixel in a grayscale image is halftoned by m subpixels.Encryption is applied to three quantized images,pixel by pixel.

4. The 3D CHAOTIC CAT MAP

Arnold cat map is one of the most studied 2D invertible chaotic maps [17], particularly in image encryption,

watermarking and steganographic algorithms. Arnold cat map is given by

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \pmod 1, \quad (1)$$

where $x_i, y_i \in [0,1]$.The map of Eq(1) is area preserving since the determinant of its linear transformation matrix A,equals 1. In [17],it is shown that the map of Eq.(1) can be generalized by introducing two new parameters a and b as follows

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \pmod 1, \quad (2)$$

Furthermore, the map of Eq.(2) can be generalized to a 3D cat map described as follows

$$X_{i+1} = \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \pmod 1, \quad (3)$$

where A is a matrix which provides chaotic behavior. A family of such matrices is given by [17].

A=

$$\begin{pmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y b_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix} \quad (4)$$

with $a_x, a_y, a_z, b_x, b_y, b_z$ all being positive integers. As a special case, let $a_x = a_y = a_z = 1$ *and* $b_x = b_y = b_z = 2$.

Thus, the map of Eq.(3) becomes

$$X_{i+1} = \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = \begin{pmatrix} 31 & 4 \\ 8311 & \\ 629 & \end{pmatrix} \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \pmod 1 \quad (5)$$

It is easy to verify that the determinant of A is equal to one and the eigen values of A are 14.3789,0.4745,0.1466.Since the leading eigenvalue is greater than 1,the map of Eq.(5) has chaotic behavior. Therefore it preserves all the features of chaos.

5. PROPOSED ARCHITECTURE

This paper combines the concepts of visual cryptography as well as chaotic encryption to implement a two-tier cryptographic system for ensuring the security of biometric templates. The proposed architecture ensures that the time and computation power for decryption procedure is minimal when compared to conventional technologies.

5.1 Generation Of Visual Cryptographic Shares

In this module the input image which is a private face image is decomposed into two independent public host images using the technique of digital halftoning, pixel expansion and encryption principle of gray-level extended visual cryptography scheme. Once two shares are obtained from the original image, for the protection and privacy of the shares which are stored in public host images, a fast image encryption algorithm based on chaos are applied on to individual shares. Here we propose an image encryption algorithm based on a 3d chaotic map.

5.2 Chaotic Encryption For Image Shares

In order to impart more security for the shares without sacrificing processing power and decryption time we can apply a chaotic encryption technique based on 3d cat map. For the protection and privacy of images we resolve to apply a two level chaotic encryption. In the first level we scramble the whole image using the generated chaotic sequences. In the second level the already scrambled image is further segmented into $S \times S$ segments. From the $S \times S$ segments, n segments are randomly selected, where $n < s^2$ by iterating a logistic map. The selected segments are further encrypted using a new set of chaotic sequences generated from the 3d chaotic map. Generation and encryption of shares are depicted in Figure.1.

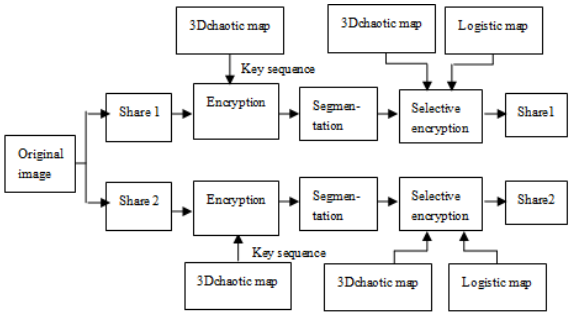


Figure. 1. Generation and encryption of shares

5.3 Chaotic decryption and re-combination of image shares

In this module the shares are recovered using suitable chaotic decryption algorithm. At first the shares are segmented into $S \times S$ segments. From these $S \times S$ segments,n segments are selected, where $n < s^2$ by iterating a logistic map using suitable keys. The selected segments are decrypted using the set of chaotic sequences generated from the 3d chaotic map. All the segments are combined and the whole image is decrypted once again done using the chaotic sequences from 3d cat map to retrieve the visual cryptographic shares. Once the decrypted shares are obtained, the two shares are overlaid using the AND operator. The process of decryption and re-combination of shares are depicted in Figure.2.

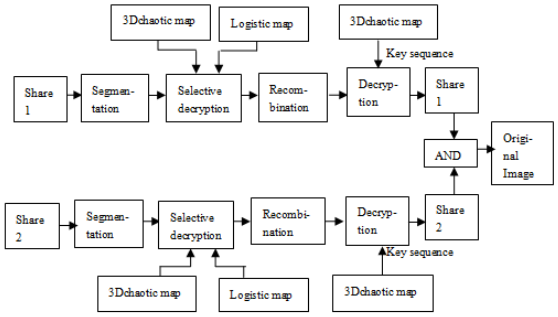


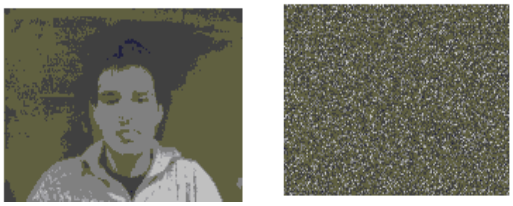
Figure. 2. Decryption and re-combination of shares

6. STATISTICAL ANALYSIS

The encrypted images should possess certain random properties in order to resist the statistical attack. In this section, we demonstrate the high security level of our suggested algorithm by showcasing its performance according to statistical analysis such as adjacent pixel correlation analysis.

6.1 Adjacent Pixel Correlation

To investigate the quality of encryption, digital simulations are performed on MATLAB. Figure.3.shows an image share and encrypted image share.



(a) (b)

Figure. 3. (a) an image share (b) encrypted image share

Since the encrypted image looks random, one would expect its adjacent pixels to have almost no correlation. On the other hand, adjacent pixel correlations are a means of measuring the performance of the algorithm. Each number in the table represents the correlation coefficient of adjacent values x_i and y_i selected at random. The covariance of x and y is defined by [17]

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu_x)(y_i-\mu_y),$$

where μ_x and μ_y are the mean values of x and y respectively. If σ_x and σ_y are the standard deviations of x and y, the correlation coefficient of x and y is defined by

$$r=\frac{\mathrm{cov}(x,y)}{\sigma_x\sigma_y}$$

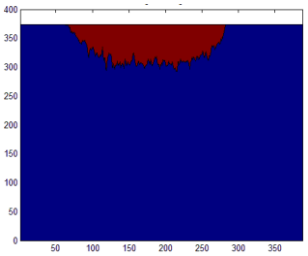
It is observed that in Table 1, there is very little correlation between pairs of adjacent pixels in the image shares and encrypted image shares.

Table 1. Adjacent pixel correlation

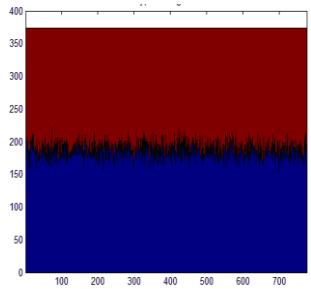
	Image share	Encrypted Image share
Horizontal	-0.30363	0.05601
Vertical	0.76741	0.68615
Diagonal	-0.30378	0.00261

6.2 Single bit test

Since the histogram analysis may not be suitable for binary images where the pixel zero and one we have adapted one bit testing for ensuring that the distribution of zero's and one's is almost uniform in the resulting image. In this test we count the number of 0's and 1's for each column of the image and plot the result. Figure.4(a). shows the plot for image share. It shows that black pixels are limited to a small portion of the image. Meanwhile in Figure.4(b) the bit counts of the encrypted image shares are uniformly distributed across all columns and also the number of one's are almost equal to the number of zero's in each column. This clearly shows the random nature of encrypted image.



(a)



(b)

Figure. 4. (a) image share (b) an encrypted image share

6.3 Key sensitivity analysis

The proposed algorithm verifies the sensitivity of the keys by encrypting the image with a triplet of keys(k_{11}, k_{12}, k_{13}) and the same image was encrypted with a new triplet of keys(k_{21}, k_{22}, k_{23}).Here the difference between k11 and k21 is 0.000001.For the two

encrypted images it was seen that the percentage of difference between the pixel values is 50.09% and thus ensuring an efficient key sensitivity. Analysis was carried out for another set of encrypted images, here also the percentage of difference between the pixel values was found to be 50.01.

7. CONCLUSION

In this paper, we use visual cryptography scheme and a 3D chaotic map to design novel security architecture for face templates. Applying Visual Cryptography scheme alone on biometric images does not lead to a complete solution for privacy as well as protection. Moreover, even if the shares have been obtained the original biometric image should not be revealed. A 3D chaotic cat map makes a suitable candidate for this purpose. Simulation results presented in this paper demonstrate that the suggested algorithm is efficient and possesses a high level of security against statistical attacks. Also a simple implementation of image encryption achieves high encryption rate on general purpose computer.

8. REFERENCES

[1] A. Jain and U. Uludag, "Hiding biometric data," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

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

[3] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22,1979, pp. 612-613.

[4] G. R. Blakley, .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[5] A.Menezes,P.Van Oorschot and S.Vanstone,Handbook of Applied Cryptography,CRC Press, Boca Raton, FL, 1997.

[6] B. Borchert, Segment Based Visual Cryptography,. WSI Press, Germany,2007.

[7] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. IEEE Transactions, ISCAS-2004, pp.572-575.

[8] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,. in Proceedings of IEEEInternational Conference on Information Technology, 2007, pp. 41-43.

[9] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, .An Innocuous Visual Cryptography Scheme,. in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.

[10] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes,. in Journal on Cryptography, vol. 12, 1999, pp. 261-289.

[11] P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with speci_ed Whiteness Levels of Reconstructed Pixels,. Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.

[12] E. R. Verheul and H. C. A. Van Tilborg, .Constructions and Properties of k out of n Visual Secret Sharing Schemes,. Designs, Codes, Cryptography, vol. 11, no. 2, 1997, pp. 179-196.

[13] H. Yan, Z. Gan and K. Chen, .A Cheater Detectable Visual Cryptography Scheme,. Journal of Shanghai Jiaotong University, vol. 38, no. 1,2004.

[14] G. B. Horng, T. G. Chen and D. S. Tsai, .Cheating in Visua Cryptography,. Designs, Codes, Cryptography, vol. 38, no. 2, 2006,pp. 219-236.

[15] C. M. Hu and W. G. Tzeng, .Cheating Prevention in Visual Cryptography,. IEEE Transaction on Image Processing, vol. 16, no. 1, Jan-2007,pp. 36-45.

[16] Fridrich J. Symmetric Ciphers Based on Two-dimensional Chaotic Maps. Int. J.Bifurcat Chaos 1998;8(6):1259-84.

[17] Chen G, Mao YB, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 2004;12:749-761.

[18] Mao YB, Chen G, Lian SG, A novel fast image encryption scheme based on the 3D chaotic baker map. Int. J. Bifurcat Chaos 2004;14(10):3613-24.

[19] Guan ZH, Huang FJ, Guan WJ. Chaos-based image encryption algorithm, Phys LettA 2005;346:153-7.

[20] Lian SG, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals 2005;26(1):117-29.

[21] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos, Solutions &Fractals, vol. 29, no. 2, pp. 393–399, 2006.

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

[23] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography fornatural images," J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.

[24] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilitiesfor visual cryptography," Theor. Comput. Sci., vol. 250, no. 1–2,pp. 143–161, 2001.

[25] S. Shevell, The Science of Color. Amsterdam, The Netherlands: ElsevierScience Ltd., 2003.

[26] R. Floyd and L. Steinberg, "An adaptive algorithm for spatialgreyscale," SPIE Milestone Series, vol. 154, pp. 281–283, 1999.

[27] A.Ross and A.Othmen, "Visual Cryptography for Biometric Privacy" ,IEEE Transactions on Information forensics and security", vol. 6, no. 1, March 2011,pp. 70-81.