ISSN 2347-4289

# Facial Template Protection Using Extended Visual Cryptography And Chaotic Encryption

**Reena Mary George**

Department of Computer Science and Engineering, TKM Institute of Technology, Kollam, India
Email: reena.mgeorge@gmail.com

**ABSTRACT:** Protection of biometric data is of prime importance now a days. In this paper a new method is proposed for the protection of biometric facial data using visual cryptography and chaotic encryption. By using visual cryptography each private face image is decomposed into two public host images. The original image gets revealed only when both of these images are available simultaneously. By using chaotic encryption extra protection as well as privacy is ensured for these images. Chaotic encryption is applied onto each share. Any system having chaotic behaviour is used for getting values for encrypting the shares. Here 1D logistic map is used.

**Keywords:** Biometry, facial image, visual cryptography, chaotic encryption, logistic map

## 1 INTRODUCTION

NOW a days biometric based personal identification Techniques are becoming more popular. Biometrics means automatic personal recognition based on physiological or behavioural characteristics. The disadvantage of traditional token based and knowledge based methods such as ID cards. and passwords is that they can be easily lost or stolen. This is not the case with biometrics since the person himself posses the biometric characteristics. For any human physiological or behavioural trait to be treated as a biometric characteristic it should possess the following properties: universality, distinctiveness, collectibility and permanence[1]. Also the biometrics technology is able to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person [2]. The biometric techniques indeed have several advantages over traditional personal identification techniques. But it has to be ensured that the security and integrity of the biometric data is preserved. The problem of using conventional algorithms such as AES, DES for the protection of biometric templates is that it takes high processing power and high encryption/ decryption time. So a new method is introduced for ensuring the security and integrity of biometric data. This method utilizes both visual cryptography and chaos-based cryptographic scheme. First the shares of biometric images are obtained using visual cryptography. These image shares are again encrypted using chaos based encryption technique. The visual cryptography scheme (VCS) was introduced by Naor and Shamir [17]. VCS is a simple and secure way to allow the secret sharing of images without any cryptographic computations. VCS is a cryptographic scheme that allows for the encryption of visual information. Here the decryption can be done by the human visual system. The basic scheme is known as the □-out-of-□ (□, □) VCS. In (□, □) VCS the encryption is done in such a way that □ or more out of the □ generated images are necessary to reconstruct the original image. Chaos theory is a scientific discipline that focuses on the study of nonlinear systems that are highly sensitive to initial conditions that is similar to random behavior, and continuous system. The properties of chaotic systems are:

(i) Deterministic, this means that they have some determining mathematical equations controlling their behavior.

(ii) Unpredictable and non-linear, this means they are highly sensitive to initial conditions. Even a very slight change in the starting point can lead to entirely different outcomes.

(iii) They appear to be random and disorderly but in actual they are not. Beneath the random behavior there is a sense of order and pattern.

The highly unpredictable and random look nature of chaotic output is the most attractive feature of deterministic chaotic system that makes it suitable to use in image encryption techniques.

## 2 VISUAL CRYPTOGRAPHY

VCS allows one to encode a secret image into sheet images, where each sheet image does not reveal any information about the original. These sheets appear just as a random set of pixels, so they may pique the curiosity of an interceptor that there might be some secret image hidden in it. To avoid this concern, the sheets could be reformulated as natural images as stated by Naor and Shamir [3]. Ateniese et al. [7] introduced a framework known as the extended VCS. Nakajima and Yamaguchi [4] proposed a theoretical framework to apply extended visual cryptography on grayscale images (GEVCS) and they also introduced a method to enhance the contrast of the target images. In GEVCS the gray-level images are transformed into meaningful binary images (halftoned images) and then applying a Boolean operation on the halftoned pixels of the two hosts and the original image.

### 2.1 Digital Halftoning and Pixel Expansion

Digital halftoning is a technique for transforming a digital grayscale image to an array of binary values. A type of halftoning technique in which the quantization error of a pixel is distributed to neighboring pixels which have not yet been processed is called Error diffusion. Floyd and Steinberg [5] 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, 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 equalling the number of subpixels per share. During the dithering process at the pixel level, any continuous tone pixel is expanded to a matrix of black and white subpixels defined by the gray level of the original pixel. Pixel transparency is defined as the proportion of white subpixels in this matrix. The host images used for encrypting a private face image as well as the private image will get converted to halftoned images.

### 2.2 Encryption

The encryption process is applied on a pixel-by-pixel basis on the three halftoned images. That means the two host images and the original image. For obtaining the required transparency (the number of white subpixels) of the target pixel the arrangement of the subpixels in the shares of both the hosts has to be controlled. The arrangement is determined based on the pixel transparencies triplet $(t_1, t_2, t_T)$.These are transparencies of the entire subpixel region for share 1, share 2, and the target, respectively. For providing security, during encryption, a Boolean matrix $B$ is randomly selected from a set of $2 \times m$ Boolean matrices $C^{t_1,t_2}$ for every pixel in the original image. The difference between this scheme[6] and Naor-Shamir's scheme is that in the latter, only a single collection of matrices is required which depends on the number of hosts and the pixel expansion.

## 3 1D Logistic Map

Logistic Map is a one-dimensional map proposed by R.M.May [8]. It represents an idealised ecological model for describing yearly variation in the population of an insect species. The population at (n+1)th year is related to that at the (n)th year by the following mathematical equation:

$$x_{n+1} = rx_n(1 - x_n) \; r \textbf{ : } \text{parameter}$$

Here $x_n$ represents the chaotic sequence which lies between zero and one[9]. When the system parameter r was varied over the interval [0,4] different scenarios of evolutionary behaviour are established. The iterates are confined to [0,1]. Depending on the value of $r$ eqn (1) has got several properties. When $r$ is between 0 and 1 the value of $x_n = 0$, independent of the value of $x_0$.When r is between 3 and 3.45 the value of $x_n$ will oscillate between two values. With slightly bigger r values the value of $x_n$ will oscillate between 4 values, then 8,16,32 etc. Like a period doubling cascade. When the value of r is 3.57 it will start exhibiting chaotic behaviour. Here slight variations in the initial condition will yield dramatically different results. Possible behaviours in the asymptotic limit, resulting out of parametric variations, are shown in Fig. 1.

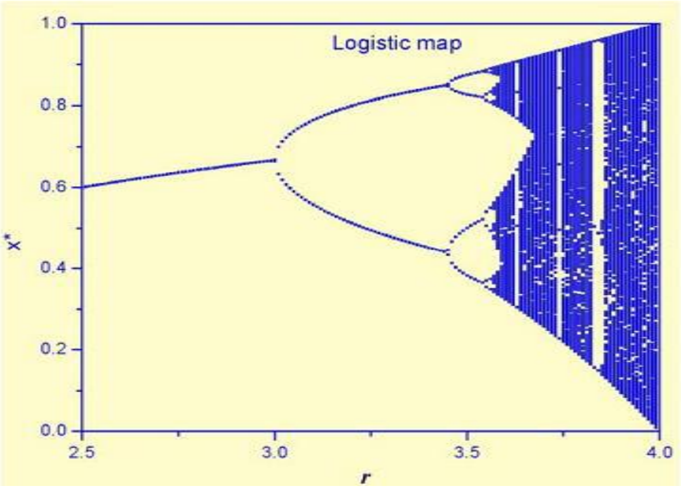

**Fig 1**.Bifurcation diagram of the Logistic map

## 4 Proposrd Architecture

In this paper the concepts of visual cryptography as well as chaotic encryption are combined to implement a two-tier cryptographic system for ensuring the security of biometric templates. The proposed architecture of the system is given in fig. 2.

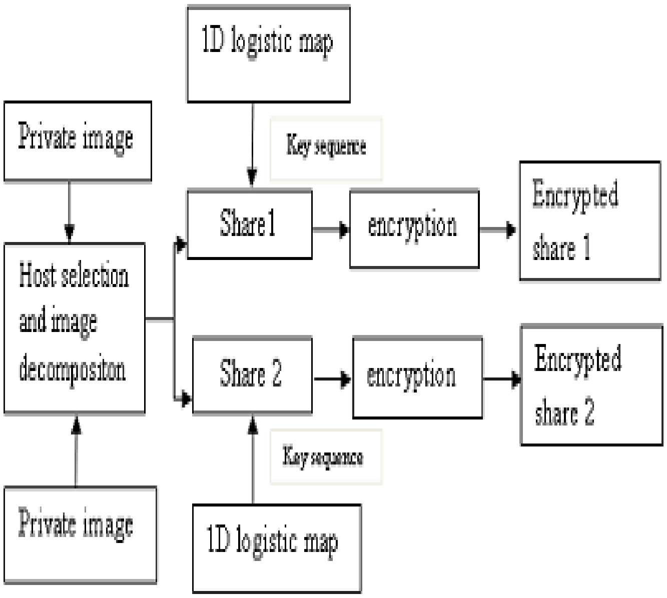

**Fig 2**.System Architecture

### 4.1 Generation of Visual Cryptographic Shares

Here the input image which is a private face image will get decomposed into two independent public host images using digital halftoning, pixel expansion and encryption principle of gray-level extended visual cryptography scheme. After the two shares are obtained from the original image, the protection and privacy of the individual shares which are stored in public host images are ensured using a fast image encryption algorithm based on chaos. Here an image encryption algorithm based on a 1d chaotic logistic map is proposed.

### 4.2 Chaotic Encryption

For providing more security to the shares we apply a chaotic encryption technique based on logistic map. Let $i$ be an image of size $M * N$. The pixel of $i$ is denoted by $i(x,y)$ where $x$ and $y$ are in the range $1 \leq x \leq M$ and $1 \leq y \leq N$. $i(x,y)$ denotes the grey value at the pixel position $(x,y)$ of image $i$ . Here the encryption is done by shuffling the pixel positions. The values for shuffling the pixel positions are got from the logistic map by iterating the equation the number of times as required. The major steps involved are :

**Step 1**: Convert the image of size M ∗ N pixels into an array $A_i = \{A_1, A_2, A_3, \ldots, A_n\}$ ,where $i = 1,2,3, \ldots, n$ and $n = M * N$.

**Step 2:** Generate n number of chaotic sequence between 0 and 1 using the logistic map mentioned in equation (1).

**Step 3:** Sort the generated elements either in ascending or descending order. Compare the misorder between the original and sorted elements of each block and tabulate the index change.

**Step 4:** According to the obtained index the intensity positions are changed to get the final encrypted image.

An example is shown in fig. 3 for a set of 9 elements. For any image this process must be done for the entire pixels in the image. The decryption process is just the reverse of encryption. The advantage of using this technique is that it is computationally less complex and it also provides faster decryption.

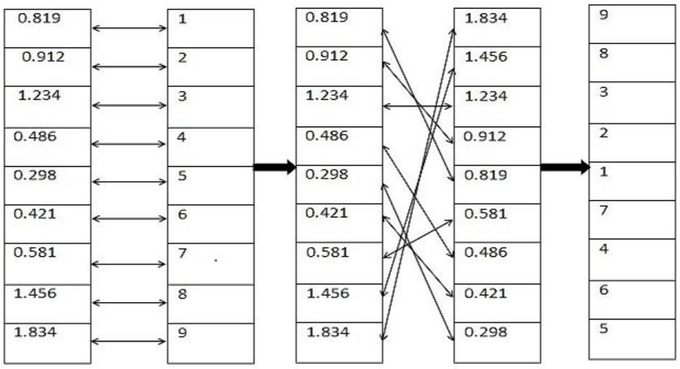

**Fig 3**. Arranging elements in descending order and calculation of displacement in index.

## 7 Conclusion

In this paper we use both visual cryptography and chaotic encryption for the protection and privacy of biometric face templates. Application of visual cryptographic scheme alone does not ensure complete privacy and protection of biometric images. That means if the shares accidentally gets into the hands of an unauthorised participant he would be able to recover the original biometric image. So the shares are again encrypted using chaotic encryption technique. Chaotic encryption is implemented using logistic map. Thus a simple and secure method to protect the biometric images is obtained through the use of visual cryptography and chaotic encryption

## References

[1] S. Prabhakar, S. Pankanti, and A. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy , vol. 1, no. 2, pp. 33–42,Mar./Apr. 2003A.

[2] Jain and U. Uludag, “Hiding biometric data,” IEEETrans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp.1494–1498, Nov. 2003.

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

[4] M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” J. WSCG , vol. 10, no. 2, pp. 303–310, 2002.

[5] R. Floyd and L. Steinberg, “An adaptive algorithm for spatial greyscale,” SPIE Milestone Series , vol. 154, pp. 281–283, 1999.

[6] 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.

[7] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, “Extended capabil-ities for visual cryptography,” Theor. Comput. Sci. , vol. 250, no. 1–2,pp. 143–161, 2001.

[8] R.M. May, “Simple mathematical model with very complicated dynamics”, Nature 261, 459(1976).

[9] Mrinal Kanti Mandal, Gourab Dutta banik, Debashish Chattopadhyay and Debashish Nandi, “An Image Encryption Process based on Chaotic Logistic Map,” IETE Technical Review, Vol 29 , Issue 5, Sep-Oct 2005.