Visual Cryptography with Chaotic Encryption for Biometric Templates

Smitha Jacob
Assistant Professor-EEE
Viswajyothi College of Engineering and Technology
Vazhakulam, Kerala, India
Email: smithatjacob@gmail.com

Mereya Baby
Assistant Professor
Viswajyothi College of Engineering and Technology
Vazhakulam, Kerala, India
Email: mereyababy@gmail.com

Abstract — Preserving the privacy of digital biometric data (e.g., fingerprint) stored in a central database has become of paramount importance. It demands high speed decryption/encryption process with restricted computational powers. This work explores the possibility of using visual cryptography with chaotic encryption suitable for imparting security to biometric data such as fingerprint images. By using visual cryptography, the original image is decomposed into two images (called shares or sheets) in such a way that the original image can be revealed only when both images are simultaneously available. The security of the stored image can be further enhanced by doing chaotic encryption to the decomposed images. Typically, a private biometric image is dithered into two host images; these images are then independently encrypted using chaotic systems and 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, Sheets are overlaid (i.e. super imposed) in order to reconstruct the private image. This work proposes a method for ensuring higher level of security for the images using visual cryptography with chaotic encryption. In the first phase of the project, the use of visual cryptography is explored to preserve the privacy of biometric data. This work is being done using Matlab 2007

Keywords- *Authentication, Key based Permutation*

*****

I. INTRODUCTION

In the existing method the use of visual cryptography with chaotic encryption is explored to preserve the privacy of biometric data (viz., raw images) by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image.

Digital technology brings us much convenience, but it also gives attackers or unauthorized users chances to access the confidential data. So if the hacker gets access to the two shares he might able to reproduce the original image since decryption process is very simple. By using visual cryptography, the original image is decomposed into two images (called shares or sheets) in such a way that the original image can be revealed only when both images are simultaneously available. The security of the stored image can be further enhanced by doing chaotic encryption to the decomposed images

II. EXISTING METHODS

For protecting the privacy of an individual enrolled in a biometric database, Matt et al. [3] and Ratha et al. [6] proposed storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template [3] or a cancellable biometric [6], Uludag et al. [11] proposed a three-step hybrid approach that combined the advantages of cryptosystems and cancellable biometrics. Apart from these methods, various image hiding approaches [10], [9] have been suggested by researchers to provide anonymity to the stored biometric data. But complicated decryption and decoding computations are used in watermarking [10], steganography [7], or cryptosystem [2] approaches.

III. SYSTEM ANALYSIS

A. Visual Cryptography

In this method the use of visual cryptography with chaotic encryption is explored to preserve the privacy of biometric data (viz., raw images) by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image. Figure.1 show block diagrams of the existing approach.

During the enrolment process, the private biometric data is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is decomposed into two

images 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 entity 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 watermarking[10], steganography[7] or crypytosystem [2] approaches. Once the matching score is computed, the reconstructed image is discarded. Further, co-operation between the two servers is essential in order to reconstruct the original biometric image.

For fingerprint image, shown in figure 1, the biometric image is decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced.

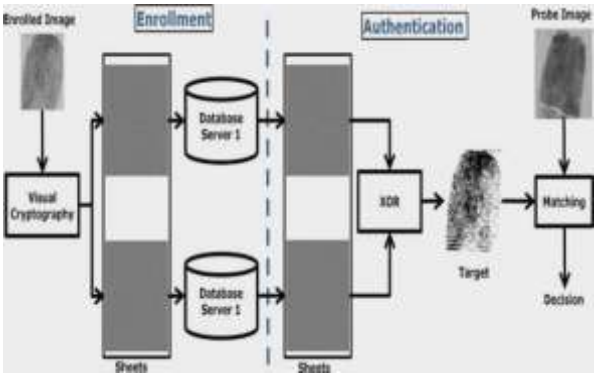

Fig. 1. Existing approach for de-identifying and storing a fingerprint image.

The first time an individual uses a biometric system is called enrolment. During the enrolment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. If enrolment is being performed, the template is simply stored within a database. Additionally, the existing approach addresses the following template protection requirements.

Diversity: For iris codes and fingerprints, the sheets appear as random noise making it difficult to match them across databases.

Revocability: If the private data is deemed to be compromised, then it can be decomposed again into two new sheets based on new host images. However, in reality, break-ins to a server are very hard to detect when the attacker simply steals certain information without modifying the stored data. To strengthen security, the decomposing operation can be periodically invoked at regular time intervals.

Security: It is computationally hard to obtain the private biometric image from the individual stored sheets due to the use of visual cryptography. Furthermore, the private image is revealed only when both sheets are simultaneously available. By using distributed servers to store the sheets, the possibility of obtaining the original private image is minimized. There have been numerous efforts in the literature to guarantee that the data stored in distributed databases are protected from unauthorized modification and inaccurate updates.

Performance: The recognition performance due to the reconstructed image is not degraded after decryption.

B. Drawbacks

Digital technology brings us much convenience, but it also gives attackers or unauthorized users chances to access the confidential data. So if the hacker gets access to the two shares he might able to reproduce the original image since decryption process is very simple.

In order to improve security using VCS one method that can be used is to increase the number of shares. But increase in number of shares needs more storage space which is a disadvantage. So a new method is needed to enhance the security of the biometric templates without increasing the number of shares.

C. Proposed Method.

Preserving the privacy of digital biometric data (e.g., fingerprint/iris images) stored in a central database has become of paramount importance. It demands high speed decryption/encryption process with restricted computational powers. This work explores the possibility of using visual cryptography with chaotic encryption suitable for imparting security to biometric data such as fingerprint images, iris codes, stored in an online environment.

Typically, a private biometric image is dithered into two host images; these images are then independently encrypted using chaotic systems and 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 entity sends a request to each server and the corresponding sheets are decrypted and transmitted to it. Sheets are overlaid (i.e. super imposed) in order to reconstruct the private image as shown in figure 2.

Cryptography is an important technique to keep private data secretly in order to avoid unauthorized access. In 1998, Baptista proposed a Chaotic Encryption Method, which seems to be much better than traditional encryption methods used . It makes use of chaotic system properties such as sensitive to initial condition and loss of information.

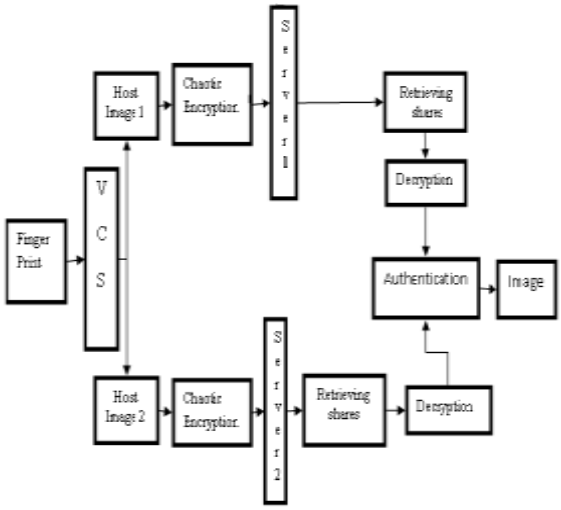

Figure 2.proposed method

Encryption is to rearrange the message into difference form so that the message is keep secret. The goal of encryption is to provide an easy and inexpensive means of encryption and decryption to all authorized users in possession of the appropriate key and difficult and expensive means to estimate the plain text without use of the key.

Key Based Random Permutation (KBRP) [8] is a method that can generate one permutation of size n out of n! Permutations. This permutation is generated from certain key (alphanumeric string) by considering all the elements of this given key in the generation process. The permutation is stored in one-dimensional array of size equal to the permutation size (N). The process involves three consecutive steps: init (), eliminate (), and fill ().

First step, init(), is to initialize array of size n with elements from the given key, by taking the ASCII code of each element in the key and storing them in the array consecutively. To complete all elements of the array, we add elements to the array by adding two consecutive values of the array until all the elements of the array are set to values. Finally, all values are set to the range 1 to N by applying the mode operation. The second step, eliminate(), is to get rid of repeated values by replacing them with value of zero and keep only one value out of these repeated values. Last step, fill (), is to replace all zero values with nonzero values in the range 1 to N which are not exist in the array. The resulted array now represents the permutation.

In second step, array P contains N values. Repetition for some values may exist; therefore, the repeated values are examined and replaced with zero. Only one value out of the repeated values is kept in P. Now P has only distinct values in the range 1 to N and some zero values are appeared in P. Missing values in the range 1 to N that are not exist in P will be substituted by the zero elements.

The final step, fill (), is to replace any zero value in P by a value in the range 1 to N which is not exist in P. All zero values will be replaced through a sequence of one value from the left side of P and one value from the right side of P and repeating this sequence until all zero values are gone. The resulted array now contains all distinct values in the range 1 to N which represents the permutation stored in P.

This approach depends on using a specific key and size in order to cover the randomness and secrecy properties for permutation. This approach is intended to use permutation in block cipher; therefore, it is suggested that a statistical test can be used to consider the permutation for the block cipher.

IV. VISUAL CRYPTOGRAPHY SCHEME

One of the best known techniques to protect data such as biometric templates 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 [4] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. The basic scheme is referred to as the k -out-of-n VCS which is denoted as (k, n) VCS [4]. Given an original binary image T, it is encrypted in n images, such that

$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \ldots\ldots \oplus S_{hk}$

where $\oplus$ is a Boolean operation, S_{hi} ,$h_i \in$ 1,2,.....,k is an image which appears as white noise, $k \leq n$, and n is the number of noisy images. It is difficult to decipher the secret image T using individual S_{hi} 's [2]. In above equation the encryption is undertaken in such a way that k or more out of the n generated images are necessary for reconstructing the original image T.

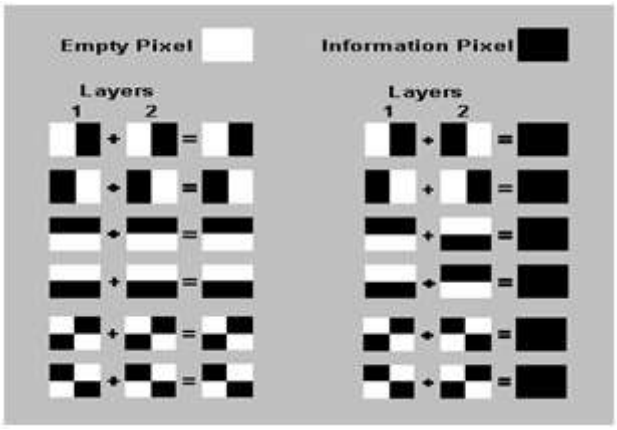

Figure 3.Subpixel Construction

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Figure. 3 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices.

When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel. Therefore, the reconstructed image will be twice the width of the original secret image and there will be a 50% loss in contrast [4]. However, the original image will become visible.

There are a few basic definitions which need to be provided before formally defining the VCS model and its extensions.

Secret image (o): The original image that has to be hidden. In our application, this is the private biometric image.

Sheets (S's): The secret image is encrypted into n sheet images.

Target (T): The image reconstructed by stacking or superimposing the sheets.

Subpixel: Each pixel P is divided into a certain number of sub pixels during the encryption process.

Pixel Expansion (m): The number of sub pixels used by the sheet images to encode each pixel of the original image.

Shares: Each pixel is encrypted by n collections of m black-and-white sub pixels. These collections of sub pixels are known as shares.

Relative Contrast (α): The difference in intensity measure between a black pixel and a white pixel in the target image.

OR-ed m-vector (V): An n×m matrix is transformed to an m –dimensional vector by applying the Boolean OR operation across each of the columns.

Hamming weight (H (V): The number of "1" bits in a binary vector V.

The k-out-of-n VCS deals with binary images. Each pixel is reproduced as n shares with each share consisting of m sub pixels. This can be represented and described by an n x m Boolean matrix B= $[b_{ij}]$ where b_{ij}=1 if and only if the jth subpixel in the ith share is black. The B matrix is selected randomly from one of two collections of n x m Boolean matrices C_0 and C_1; the size of each collection is r. If the pixel P in the secret image is a white pixel, one of the matrices in C_0 is randomly chosen; if it is a black pixel, a matrix from C_1 is randomly chosen.

Upon overlaying these shares, a gray level for the pixel P of the target image becomes visible and it is proportional to the Hamming weight (V), of the OR-ed- m-vector V for a given matrix. It is interpreted visually as black if H (V) ≥ d and as white if H (V) < d - αm for some fixed threshold 1≤ d ≤ m and relative difference α > 0. The contrast of the target is the difference between the minimum H (V) value of a black pixel and the maximum allowed H (V) value for a white pixel, which is proportional to the relative contrast (α) and the pixel expansion (m).

The scheme is considered valid if the following three conditions are satisfied. **Condition 1**: For any matrix B in C_0 , the OR operation on any k of the n rows satisfies H (V) < d - αm. **Condition 2:** For any matrix B in, the OR operation on any k of the n rows satisfies H (V)≥ d. **Condition 3**: Consider extracting q C_0 rows, q< k, from two matrices B_0 € C_0 and B_1 € C_1 resulting in new matrices $B_{0'}$ and $B_{1'}$. Then, B_0'and B_1'are indistinguishable in that there exists a permutation of columns of B_0' which would result in $B_{1'}$. In other words, any q x m matrix B_0 € C_0 and B_1 € C_1 and are identical up to a column permutation.

Conditions 1 and 2 define the image contrast due to VCS. Condition 3 imparts the security property of a (k, n) VCS which states that the careful examination of fewer than k shares will not provide information about the original pixel P. Therefore, the important parameters of the scheme are the following. First, the number of sub pixels in a share (m); this parameter represents the loss in resolution from the original image to the resultant target image and it needs to be as small as possible such that the target image is still visible. In addition, the m sub pixels need to be in the form of a v x v matrix where v € N in order to preserve the aspect ratio of the original image. Second, α, which is the relative difference in the Hamming weight of the combined shares corresponding to a white pixel and that of a black pixel in

the original image; this parameter represents the loss in contrast and it needs to be as large as possible to ensure visibility of the target pixel. Finally, the size of the collection of C_0 and C_1 , which represents the number of possibilities of V. This parameter does not directly affect the quality of the target image.

A. Encryption

The use of basic visual cryptography for securing fingerprints was suggested by Singh et al [9]. To encode the finger print image (2, 2) VCS is used [1]. Each pixel in the original image is encrypted into two sub pixels called shares. The coding was done using Mat lab and a GUI screen is used for the control and manipulation of the process. Encrypted image is shown in figure 4.

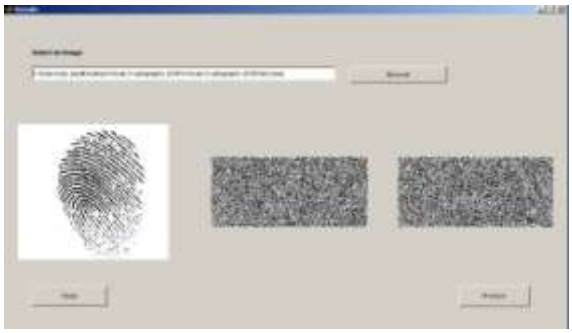

Figure 4. Encrypted Images

B. Decryption

Images can de decrypted using OR or XOR function. Only when we get two shares of the same image we can reproduce the original image. Two option button named as OR and XOR are also provided on the screen So as to facilitate and analyse the results obtained using these two methods. Based on the indicated button OR or XOR processing is done

.

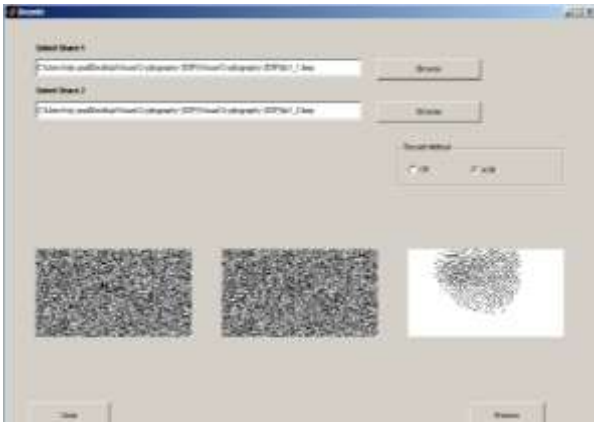

Figure5.Decryption using XOR

V. RESULT ANALYSIS

The overlaying or superimposing operation in visual cryptography is computationally modeled as the binary OR operation which causes the contrast level of the target image to be lowered. Loss in contrast in target images could be addressed by simply substituting the OR operator with the XOR operator [12]. Furthermore, the target image can be down-sampled by reconstructing just one pixel from every block. Thus, the reconstructed image will be visually appealing while requiring less storage space. It is clearly evident that the contrast of the original image is restored in the latter.

The reconstructed as well as the original grayscale fingerprint probes were matched against the impressions in the gallery. Using the original fingerprint images as probes resulted in an EER of 8%. It is observed that a threshold of 180 results in an EER of 9.13%. These experiments suggest the possibility of decomposing and storing fingerprint image using VCS.

VI. CONCLUSION AND DISCUSSION

Biometric authentication, i.e. verifying the claimed identity of a person based on physiological characteristics or behavioral traits, has the potential to contribute to both privacy protection and user convenience. From a security point of view, biometric authentication offers the possibility to establish physical presence and unequivocal identification. However from a privacy point of view, the use of biometric authentication also introduces new problems and user concerns. When used for privacy-sensitive applications, biometric data are a highly valuable asset. When such data are available to unauthorized persons, these data can potentially be used for impersonation purposes, defeating the security aspects that are supposed to be associated with biometric authentication. In this work a method for ensuring higher level of privacy for the images using visual cryptography with chaotic encryption is proposed. It also provides high speed decryption/encryption process with restricted computational power. In this phase of the project visual cryptography is done on the image. Both encryption and decryption of the image is done. In the future work of the project the enhancement of the security with chaotic encryption is to be done.

REFERENCES

[1] Arun Ross, Asem Othman," Visual Cryptography for Biometric Privacy" IEEE Trans. On Information forensics and security, vol.6, no.1, March 2011.

[2] Jain. A, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Advances Signal Process, pp. 1–17, June 2008.

[3] Matt. B. J, Davida. G I, and Y. Frankel, "On enabling secure applications through off-line biometric identification," in Proc. IEEE Symp.Security and Privacy, pp. 148–157, May 1998.

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

[5] Pankanti. S, Jain. A. K and A. Ross, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, June 2006.

[6] Ratha .N, J. Connel, and R. Bolle, "Enhancing security and Privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614– 634, August 2001.

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

[8] Shakir M. Hussain and Naim M. Ajloun " Key Based Random Permutation (KBRP)" Journal of Computer Science 2 (5): 419-421, ISSN 1549-3636, April 2006.

[9] Singh. U, Y. Rao, Y. Sukonkina and C. Bhagwati, "Fingerprint based authentication application using visual cryptography methods (improved ID card)," in Proc. IEEE Region 10 Conf., pp.1–5, Nov 2008.

[10] Tan. T and Dong. J, "Effects of watermarking on iris recognition performance," in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, (ICARCV 2008), pp. 1156–1161, July 2008.

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

[12] Yan. W. Q, D. Jin and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag. vol. 14, no. 3, p. 033019, May 2005.