Multilevel Security in Face Authentication

Deepak.A, Amrita.A.Manjrekar

Abstract— The security and trust in using biometrics as a mean to verify the authenticity entirely lies in preserving the privacy of digital biometric data (e.g., face images) stored in a central database. The possibility of using visual cryptography and steganography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images is explored. The biometric information such as the private face image is decomposed into two host face images (known as sheets, shares or transparencies) that are stored in two separate database tables such that the private image can be revealed only when both sheets are simultaneously available, and the individual sheet images do not reveal the identity of the private image. In order to provide an extra level of security, the concept of steganography is also included in the proposed project. The username and password which is used for the authentication of the user is stored in a hidden format using steganography. The username and password are stored in the transparencies of the face image. The combination of biometrics, visual cryptography and steganography in the proposed system with mutually interconnected security mechanism provides the best authentication system.

Index Terms— Authentication system, Biometrics, Pixel division, Security, Shares, Steganography, Visual Cryptography.

1 INTRODUCTION

THE Biometrics or biometric recognition refers to the identification of humans based on physical or behavioural traits or characteristics such as face, fingerprints, iris, gait and voice. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. 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 a claimed identity[1].

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioural characteristics. A physiological biometric would identify by one's voice, DNA, hand print or behaviour. Behavioural biometrics is related to the behaviour of a person, including but not limited to: typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

Many different aspects of human physiology, chemistry or behaviour can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. It is identified that seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. **1) Universality:** means that every person using a system should possess the trait. **2) Uniqueness**: means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. **3) Permanence:** relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm. **4) Measurability (collectability):** relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. **5) Performance:** relates to the accuracy, speed, and robustness of technology used (see performance section for more details). **6) Acceptability:** relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. **7) Circumvention:** relates to the ease with which a trait might be imitated using an artifact or substitute.

In this paper, the use of visual cryptography 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. 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 steganography, or cryptosystem 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.

2 VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data such as biometric templates [4] 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 [3] 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. Given an original binary image, it is encrypted in images, such that $T=S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \ldots\ldots S_{hk}$ where $\oplus$ is a Boolean operation, S_{hi} , $h_i \in 1,2,\ldots k$ 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 using individual S_{hi}'s. 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.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. 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. However, the original image will become visible.

2.1 Grey Level Extented Visual Cryptographic Schemes (GEVCS)

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 [3]. Nakajima and Yamaguchi [8] proposed a theoretical framework to apply extended visual cryptography on gray scale 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.

3 Related Works

Protection of biometric data and templates is a crucial issue for the security of biometric systems, and biometric watermarking is introduced for this purpose [4]. However, watermarking introduces extra information into the biometric data (biometric images or biometric feature templates) which lead to certain image distortion. In addition, watermarked images are always subject to the risk of being attacked. Hence, whether and how biometric recognition performance will be affected by biometric watermarking deserves investigation. Introduced two application scenarios in the context of iris recognition, namely protection of iris templates by hiding them in cover images as watermarks (iris watermarks), and protection of iris images by watermarking them. They found out that watermarking iris images does not introduce detectable decreases on iris recognition performance whereas recognition performance drops significantly if iris watermarks suffer from severe attacks.

Ratha *et al.*[5] explains several problems that are unique to biometric authentication systems and propose solutions to many of those problems. This paper mainly focuses on finger print recognition as a model but the concepts and solutions can be extended for the analysis of other biometric authentication methods. Methods are proposed for preserving the privacy of the individuals enrolled in the biometric database. This method used a technique of storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template or a cancellable biometric. The transformation made by adding a series of noise pixels into the biometric template.

Davida *et al.*[6] discuss about secure offline authenticated user identification schemes based on a biometric system that can measure a user's biometric accurately (up to some Hamming distance). The schemes presented here enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as a magnetic strip. Schemes are also developed specifically designed to minimize the compromise of a user's private biometrics data, encapsulated in the authorization information, without requiring secure hardware tokens. It also studies the feasibility of biometrics performing as an enabling technology for secure system and application design.

The Active Appearance Model (AAM) concept [7] show an efficient direct optimization approach that matches shape and texture simultaneously, resulting in an algorithm that is rapid, accurate, and robust. This method does not attempt to solve a general optimization problem each time to fit the model to a new image. Instead, it exploits the fact that the optimization problem is similar each time so that it can learn these similarities offline. This allows finding directions of rapid convergence even though the search space has very high dimensionality. It also described a method of matching statistical models of appearance to images. A set of model parameters, control modes of shape and gray-level variations are learned from a training set.

In [8], Extended Visual Cryptography is discussed which is a type of cryptography that encodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is done directly by the human visual system with no special cryptographic calculations. This paper presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. While the previous researches basically

handle only binary images, the extended visual cryptography scheme is suitable for natural images. Generally, visual cryptography suffers from the deterioration of the image quality. Extended visual cryptography also describes the method to improve the quality of the output images. The trade-off between the image quality and the security are discussed and assessed by observing the actual results of the extended VCS method.

4 Proposed System

With the availability of modern high performance hardware and latest software technologies, the security of any system can be easily breached and compromised. In such a situation the one and only one option which provides a higher degree of security is biometric authentication methods. Even if biometric authentication is capable to prevent the unauthorized access to the system, it does not guarantee that the authentic person can always access a system with ease even if an intruder modified or altered the secret database of the authentication system. To avoid this problem the most common method of image encryption technique that is visual cryptography is employed together with the biometrics. The proposed system shown in Fig.1 provides a high level of security as compared to other traditional authentication systems.

4.1 Components of Proposed System

In this proposed system, the use of visual cryptography 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. The proposed project has three significant components.

4.1.1 Public Host Image Database

The use of face images as hosts for a private face image (as opposed to using random noise or other natural images) has several benefits in the context of biometric applications [2]. The demographic attributes of the private face images such as age, gender, ethnicity, etc. can be retained in the host images thereby preserving the demographic aspects of the face while perturbing its identity. Alternately, these demographic attributes, as manifested in an individual's face, can also be deliberately distorted by selecting host images with opposite attributes as that of the private image. A set of public face images (e.g., those of celebrities) may be used to host the private face database. That is, a small set of public images can be used to encrypt the entire set of private face images. Using non-face images as hosts may result in visually revealing the existence of a secret face. While decomposing the face image into random noise structures may be preferable, it can pique the interest of an eavesdropper by suggesting the existence of secret data.

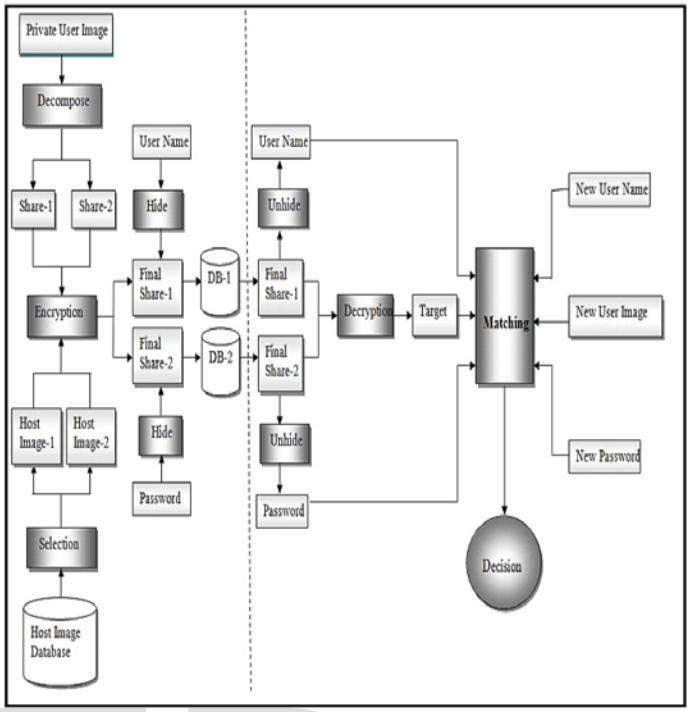


Fig.1 Architecture of the proposed approach

4.1.2 Trusted Third Party Entity

The trusted third party is a component which is capable of performing both storing and decomposing of the image that has to be stored in the biometric database. The image which has to be stored in the database is taken either with a camera present along with the system or it is manually stored by capturing the image by an external digital camera. The image input in the previous step is temporarily stored in a database table until it gets encrypted in the next step. The image is decomposed into two different images or shares and the initial image is discarded. Two face images stored in the host database are selected. The face image decomposed in the step 3 is encrypted pixel by pixel using the two host images selected from host database. The two shares are moved to two different database tables. During authentication phase the image of the person who is trying to access the system is taken with the help of a camera (webcam). The trusted entity sends a request to each database tables. The corresponding sheets are transmitted to the third party entity. Sheets are overlaid (i.e., superimposed) to reconstruct the private image. Once the matching score is computed, the reconstructed image is discarded. If the image reconstructed is matching with the newly taken image, then authentication is provided to that particular user.

4.1.3 Steganographic Componente

The proposed system provides an added security by employing steganographic techniques. The commonly used Username and password system of authentication is modified in this method. Normally the username and password are stored as such in the database, here in this system the user name and password are kept hidden in the transparencies of

face image generated in the previous stage. This is done using LSB steganography technique.

4.2 Selection of Host

The selection of compatible hosts, for encrypting the private face image is done such that the user face image can be completely kept hidden securely inside the host image. Both the user image and the host image selected must be of compatible size. That means, the length and breadth of both the images must be at the most equal or the size of the host image should be greater than the user image. Any situation in which the user image is greater than the public host image will results in an exception or error. The resolution or quality difference in the user image and public host image does not have any sort of impact in the accuracy of result. Because of this technique, it is able to hide the user image behind the host image without making any trace of existence of one secret image visible to the external viewer.

In [2] the selection of the cover image from the public host image database is purely based on a factor called registration cost or transformation cost. Transformation Cost (T_c) is the cost of registering (aligning) each image in the public dataset with the private image. These costs are sorted in order to locate two host images, and the host images for which the transformation cost is the smallest will be selected. Obviously the reason for avoiding such a technique for host image selection is the higher computational time. Apart from higher computational time, it also increases the load of the system as it requires the comparison of a single user image with as much images present in the host image database. Because of the reason of higher time and space complexity, the above mentioned method is completely avoided in this system and is replaced by a random selection criterion as required by the administrator or trusted third party.

4.3 Algorithms for Facial Image Encryption

The sequence of steps followed for the encryption of a face image is summarized here. At first the private face image which has to be encrypted is entered into the system with the help of a camera attached to the system or by loading a digital image which is already stored in the system. Next select two face images from the public host image database. Selection of host image is done randomly or as desired by the trusted third party. After selecting two host images (H_{s1} H_{s2}) they are aligned with the face image O. In the next step the aligned host and private images are cropped to capture only the facial features. Then encrypt the facial image in host images H_{s1} and $H_{s2,}$ using Grey-level extended visual cryptography scheme resulting in shares S_1 and $S_{2..}$ The Grey level extended visual cryptography has different stages within it. Initially consider three pixels at a time, such that one pixel is from the secret image ant the remaining two pixels are from the host images. Divide the pixels into sub pixels using pixel expansion method. Determine the triplet $t_{1,}$ $t_{2,}$ and $t_{T,}$ where t_1 and t_2 are the pixels in the share and t_T is the target pixel. t_T is the target pixel constructed by the combination of pixels $t_{1,}$ and $t_{2,}$ Construct the collection matrix C. C is a set of xm Boolean matrices where m is the pixel expansion. Select matrix B from C for encoding each pixel. Superimpose the shares S_1 and S2 to retrieve the actual secret face image.

4.4 Algorithms for Steganography

The principle of steganography is to hide one message within the other without modifying the actual message. Usually an image is used as the cover image and a text is used as the information to be hidden. The LSB [12] based steganography have five different steps. Firstly the cover image is read from the user and the text message which has to be hidden in the cover image. Secondly convert the text message into binary format. In the third step calculate the least significant bits of each pixels of the cover image. In the next step replace the least significant bits of the cover image with the each bit of secret message one by one. And finally write the steganographic image.

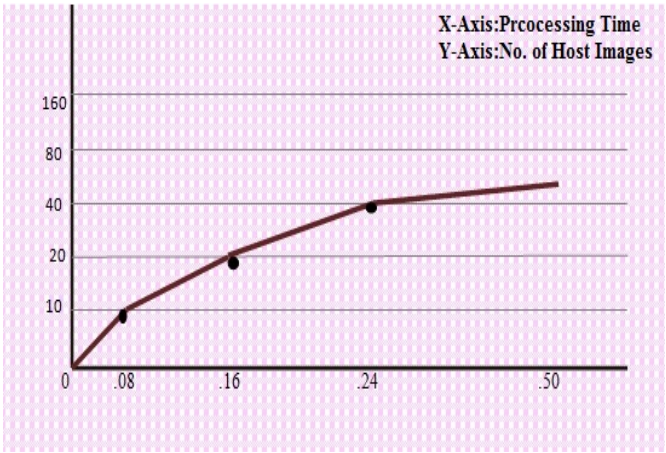
5. Experiments and Results

5.1 Experiment 1

In this experiment, the impact of varying the number of images in the host image database was investigated. The selection of hosts from the public dataset was based only on the similarity level. The image with maximum dissimilarity is considered as the cover image. It is found out that as the number of images present in the host image database increases, the performance and accuracy of system increases up to a level. But when the host image database is very much populated then it negatively affects the system by increasing the performance overhead on calculating the similarity level of the private image with each of the host images.

Fig 2 Host Image Number Versus Performance Time

5.2 Experiment 2



The purpose of this experiment was to determine if the encrypted face images upon reconstruction could be successfully matched against the original private face images. For this, the different face images of same individual with different head rotations angles are taken. Out of these, the facial images in which the facial features are clearly visible can be accurately matched with the reconstructed image. If the facial

features are not visible, i.e. the angle of head rotation is more than 30 degree, in that case the similarity level drop down nearly about 35 to 50 on average.

5.3 Experiment 3

In this experiment the effect of change in angle of rotation is calculated. A set of images of same person are selected from the IMM database. Out of the images, some image does not reveal the facial features correctly because of rotation. In such cases the matching gives a similarity value very less than that of the acceptable threshold value. So it is found that image capture must be done such a way that all the facial character is properly and completely captured in the image.

Fig 3 Enrolled Image

Fig 4 Images with Facial Angle Rotation

User Images	Similarity Level With Enrolled Image
	0.928446
	99.981278
	3.194387
	100

5.4 Experiment 4

This experiment verifies the possible methods of attacks that are likely to occur in this system during a cryptanalysis process. In normal cryptography, the cryptanalysis process is mainly classified based on the data the attacker possess and used for decrypting the hidden information. The possible methods of cryptanalysis are as follows.

Known cipher text only

Consider the first type of cryptanalysis with known cipher Text. As the system deals with images the cipher data (the data after encryption) is also in the form of images. In this scenario, an attacker knows a cipher data means that the attacker is having either of the two final shares generated by the encryption of the initial share with the randomly selected host image. since the data base contains different shares encrypted with same host image, it is difficult to find the corresponding user from the obtained cipher data (final share). It is also impossible to find out the matching pair of cipher data from another database.

Known plain text only

In this system the plain text corresponds to the facial image of the user. Suppose that the plain text is known to the attacker. If an attacker knows the exact facial feature of a user and disguise as genuine user, then the system shows proper matching between the genuine user and the attacker. But the attacker cannot get complete success over the system as this system provides multilevel security and it requires the matching of other details such as user name, password and primary key. If the attacker only knows the user name, password and primary key then also the system will not provide access as the facial features are not getting matched.

6 Conclusion

This paper explored the possibility of using visual cryptography for imparting privacy to biometric templates. The contribution of this project includes a methodology to protect the privacy of a face database by decomposing an input private face image into two independent sheet images such that the private face image can be reconstructed only when both sheets are simultaneously available. The algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. GEVCS is then used to encrypt the private image in the selected host images. This helps to avoid the chance for revealing the existence of a hidden image in the host image. It is observed that the reconstructed images are similar to the original private image. The application of steganography provides the added security. The textual details are kept hidden in the individual shares so it acts a multilevel security mechanism that exhibits a synergic effect as a whole. Finally, experimental results demonstrate the difficulty of exposing the identity of the secret image by using only one of the sheets; further individual sheets cannot be used to perform cross-matching between different applications. This system can be used with ease in several application areas such as ATM counters, electronic voting systems, banking sector etc.

References

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

A.Ross and A.Otheman, "Visual cryptography for biometric privacy", IEEE Trans. Information forensic and Security, vol. 6, no. 1, march 2011

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

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

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.
G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in Proc. IEEE Symp. Security and Privacy, 1998, pp. 148–157.
T. Cootes et al., "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, Jun. 2001.
M. Nakajima and Y. Yamaguchi, Extended Visual Cryptography for Natural Images.
Debasish Jena and Sanjay Kumar Jena. "A Novel Visual Cryptography Scheme," IEEE 2008.
A.Incze, "Pixel Sieve Method of Visual Cryptography," in Proc. IEEE Symp. Security and Privacy March 2009
Lisa M. Marvel, Charles G. Boncelet and Charles T. Retter, "Spread Spectrum Image Steganography" IEEE Transaction on Image Processing, Vol. 8, no. 8, August 1999
M. B. Stegmann, B. K. Ersb¿ll, and R. Larsen. FAME- A Flexible appearance modelling environment. *IEEE Trans. on Medical Imaging*, 22(10):1319-1331, 2003
Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, "Fingerprint based authentication application using visual cryptography methods (improved id card)," in *Proc. IEEE Region 10 Conf.*, Nov. 2008, pp. 1–5.
P. Revenkar, A. Anjum, and W. Gandhare, "Secure iris authentication using visual cryptography," *Int. J. Comput. Sci. (IJCSIS)*, vol. 7, no. 3, pp. 217–221, Mar. 2010.
Shailender Gupta " Information Hiding Using Least Significant Bit Steganography and Cryptography" *I.J.Modern Education and Computer Science*, 2012, 6, 27-34