ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Study on Multitier Biometric Authentication using Cryptography with Fingerprint and Eyelashes

Ms. Saranyadas S[1], Dr.A.Nithya[2]

Research Scholar, Department of Computer Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Dept. of Computer Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: Security on an Automated Teller Machine (ATM) is the major issue in the current world. Improving the security is necessary to customer's transaction protection. So the best solution for security and authentication is biometric system, it offers convient and secure mode of authentication to the user numbers of threatens are there hacking of password etc all of them have the solution is biometric. Authentication is a critical part of trustworthy computing system, which want to ensure to the customer that only individuals with corroborated identifiers can log on to the system or access the resource. The biometric authentication with cryptography improves the security level of authentication. In this paper propose a bio-metric system for encrypting the user password is for secure ATM transaction. A fingerprint and eyelash image is required at transaction time. Then it will compare with server database only further transaction will allow matching occur with server database.

Keywords: Biometric, Authentication, Cryptography, Finger print , Eyelashes, Automated Teller Machine, Security, Harris Corner Detection ,Encryption, Decryption.

1. INTRODUCTION

In many area using bio-metric system for authentication. It offers several advantages over other authentication methods. Mainly to avoid the attacks hacking etc. Here it is using on to the banking section ATM for quick money withdrawal.

Most of the banking system using authentication and security for money withdrawal on ATM is PIN (Personal Identification Number)or password. But now days this digits or password will easily hacked by others. By using biometric concept can overcome this problem.

The present work aims at authentication on ATM by using '***eyelash'*** and '***fingerprint'***. Eyelash and fingerprint both are unique structure and shape for each individual that why here using the new implement as eyelashes. How many hair will fallen down daily and that much will be after within somedays, but never change.

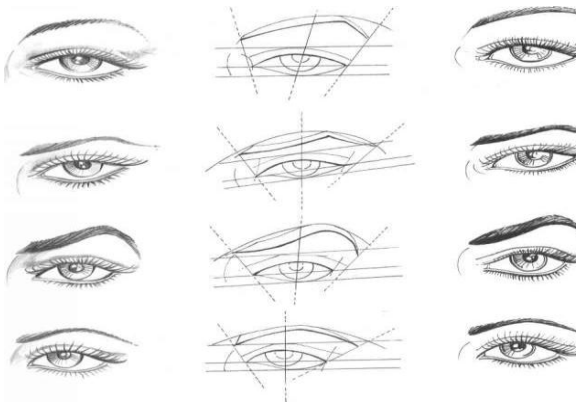


FIG: 1

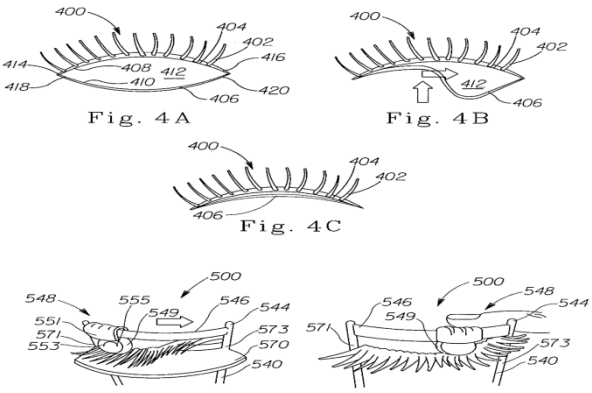


FIG: 2

At the time of transaction fingerprint and eyelash image is acquired at the ATM terminal using high resolution eye tracker and for fingerprint scanning using Derma log LFIO Ten print Scanner ,then 256 bit bio key is generated from the selective feature point extracted from the image using Harris corner detection[1] user's password method using bio-key. Then it will transfer or send to the server for checking. Success of authentication based on the matching process.

In the Harris corner detector [2] is used to detect the corners in eyelash images as bio-metric system. The algorithm is based on the local auto-correction function of a signal. The local auto-correction function measures the local changes occur small difference. Some selected pixel is position value of corner based only the bio key is generated. Each and every human being has unique eyelash structure.

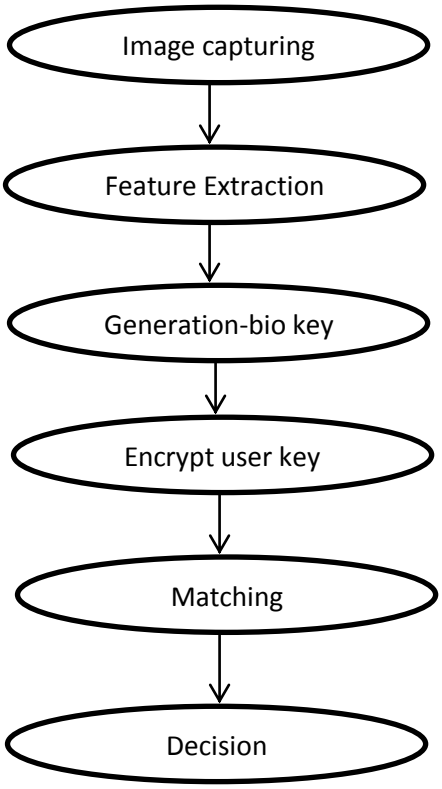
DOI 10.17148/IJARCCE.2015.4858

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

2. METHODOLOGY

In this paper using methodology is that, the user are allow to give the combination of various biometric concepts for their identity and authentication. Mainly in biometric system including several steps they are [2]



Bio –metric concept working methodology

A. Image Capturing

It is the first step in any biometric concepts, while transaction time at ATM terminal, will capture the image of (eyelash) eye by using eyetracking and also scan the fingerprint.

B. Feature Extraction

In this step features of various biometrics are extracted by applying the algorithm. Here the Harris corners algorithm apply and taking the corners from the image. So the image will converted as greyscale and pre-processed gray image than extract the structure and length of the eyelashes with the corner points.

C. Bio-key generation

Based on the feature extraction and applying Harris corner will get corner,based on the corner will generate a bio-key.

D. Password Encryption

Then the user password will encrypt and also combine with the bio-key. It will transfer to the matching section.

E. Matching

Matching mean the feature value extracted at present compare with the server database. Matching result is positive mean only allow to further process else show access denial.

F. Decision

It is the final stage, show access denial or access granted only matching result positive

3. RELATED WORK

There are number of biometric system used to security and authentication for ATM. In India using the biometric system for authentication is very low. But in the other countries like US, UK, Japan are using wide range of biometric technologies in their banking and finance area. In Japan bank ATM's are running with palm vein recognition [2]. Bank of Columbian bane cafe ATM using fingerprint [2]. Many authors are related work of biometric concept with different algorithm.

Table: 1 Different types of bio-metric concept[2]

Biometric	**Pre-processing techniques**	**Distinctive patterns**
Finger	Binarisation Segmentation Enhancement Minutiae extraction Orientation Thinning	Minutiae points: ridge ending Bifurcation Cross over Island Delta
Iris	Segmentation Normalization Extraction of iris textures	Rings Furrows Freckles Corona
Face	Face location Face recognition	Eye socket open ridge Cheekbone area Nose shape Mouth points
hand	Binarisation Segmentation Enhancement Morphological operations	Finger width Finger height Hand bone structure Joints distance

4. PROPOSED ALGORITHM

In computer vision, usually we need to find matching points between different frames of an environment. If we know how two images relate to each other, we can use both images to extract information of them .When we say matching points we are characteristics in the scene that we can recognize easily. We call these characteristics features. The characteristics should must be uniquely recognizable. So here using Harris corner detection [1].

Harris Corner Detection Algorithm Calculation

1. Compute x and y derivatives of image

$$Ix=G^{x}_{\sigma}*I \quad Iy=G^{y}_{\sigma}* I$$

2. Compute products of derivatives at every pixel

$$Ix_2=Ix . Ix \quad Iy_2=Iy .IyIxy=Ix .Iy$$

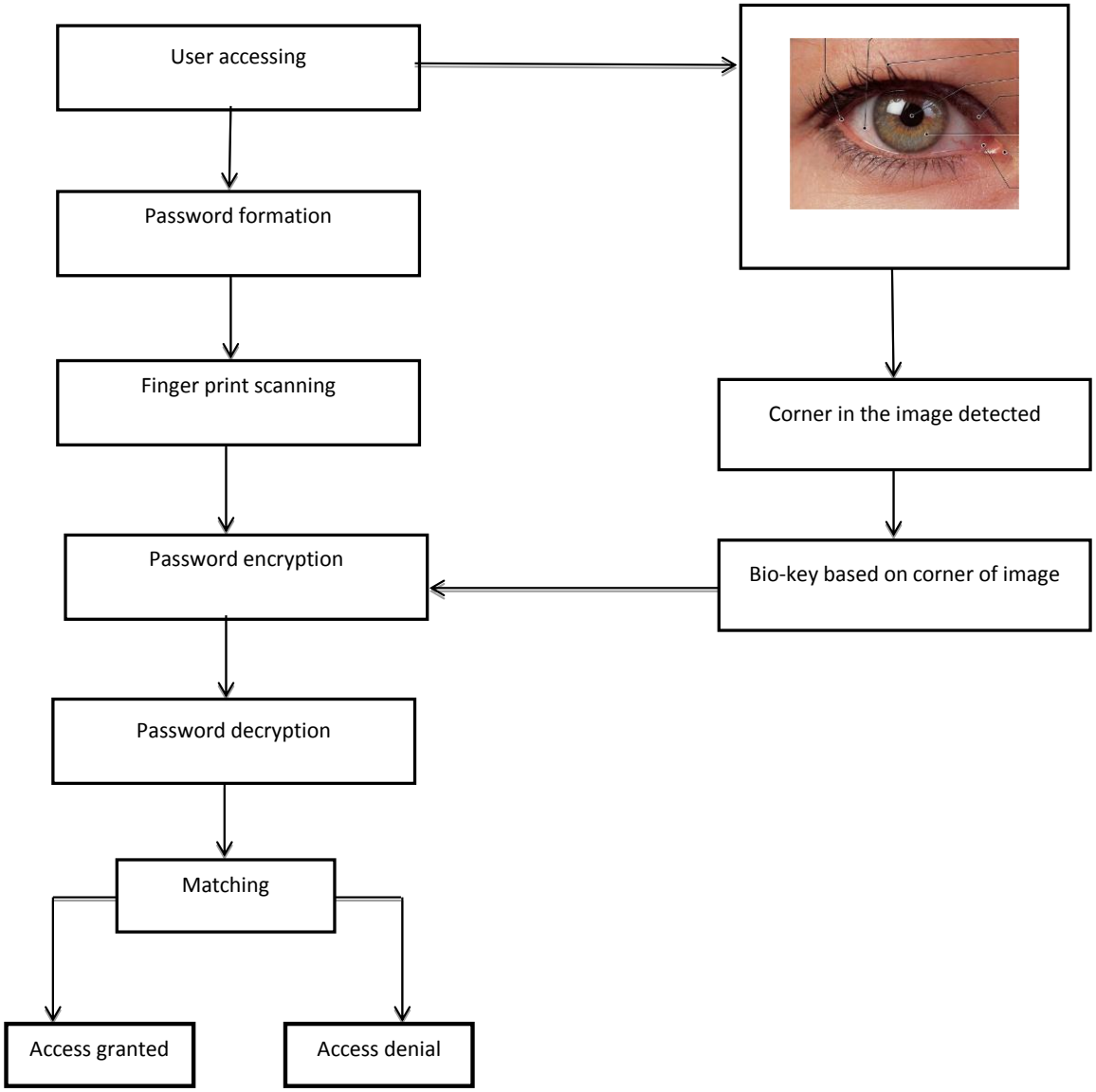
3. Compute the sum of the products of derivations at each pixel

$$Sx2=G_{\sigma 1}* I \quad Sy2=G_{\sigma 1} * Iy2 \quad Sxy=G_{\sigma 1} * Ixy$$

DOI 10.17148/IJARCCE.2015.4858

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015



Working model[1]

4. Define at each pixel (x,y) the matrix

$$H(x,y)=\begin{bmatrix} Sx2(x,y) & Sxy(x,y) \\ Sxy(x,y & Sx2(x,y) \end{bmatrix}$$

5. Compute the response of the detector at each pixel

$$R=Det(H)-K(Trace\ (H))^2$$

6. Threshold on value of R compute nonmax suppression

Mainly the three Eigen values are consider in the Harris corner And it is also feature of an image

1) Both Eigen Values are small signifying common region (constant intensity)
2) Both values are high signifying point (corner)
3) Only one values is high signifying contour (edge)

To find out these points of interest, characterize corner response

- H(x , y) by Eigen Value C(x , y)
- C(x , y) is symmetric & a positive that is α1 &α2 are > 0
- α1 α2=det (C(x,y)) =AC-B2
- α1 +α2=trace (C(x , y))=A+C
- Harris suggest corner response

It is H response = α1 α2-0.04 (α1 + α2)2 it need to findout corner points as local maxima of the corner response.

4.1 PROPOPSED METHOD

Key generation from the eyelash image

Step 1: Colored eye image converted into grey scale by green channel [1].
Step 2: From grey scale image pre-processed feature to extract eyelash structure.
Step 3: Then the image is binarized.
Step 4: Applying the Harris corner detection algorithm.
Step 5: Calculate all Harris corner detected.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Step 6: First 8 Harris corner position into 8bit binary generate a bio-key [1].

4.2 PASSWORD ENCRYPTION

Step 1: Converting the 8 character password into 8*8 binary matrixes and converting individual 8bitbinarized ASCII values.
Step 2: Bio-key matrix will generate [1].
Step 3: Generate password matrix.
Step 4: Based on the bit position select password matrix first row.
Step 5: Calculate Hamming distance between the groups of corners
Step 6: Based on the Hamming value matrix will modified
Step 7: Calculate the ASCII value and only the 2 bit of the decimal will allow (eg: .655 as 65).
65 represent as 'A'
Encrypted value 655 is 'A5'
Step 8: Decryption algorithm applied and the reverse order for password encryption to recover the password [1].

5. CONCLUSION

In this paper a new biometric system for ATM authentication proposed. While transaction time at ATM need the image of eye (eyelash) and fingerprint also, later it will converted into grey scale image and apply Harris corner detection to find out the corner, based on that make a bio-key and user password encrypt and analyze the fingerprint. Both biometric system eyelash and fingerprint matching server database only further process will grant [1].

FUTURE ENHANCEMENT

In the future many technologies will used to improve security at ATM than this and now this approach is a unique from already available or used. It will provide more secure than other and in future more technologies will add on to the work.

REFERENCES

[1]. "A biometric authentication based secure ATM banking system" by Shouvik Biswas,Anamritha Bardhan,Kishore Ghosh,Nilanjan Dey.
[2]. "A comparitive study on ATM security with multimodal biometric system" by K.Lavanya and C.naga Raju.
[3]. "Multitier biometric template security using cryptographyic salts and personal image identification" by Sarika Khandewaland P.C.Gupta.
[4]. "ATM security using fingerprintbiometric identifer an investigative study" by Moses Okechukwu Onyesolu and Ignatius MajestyEzeani.
[5]."Cryptography based authentication methods" by Mohammad A.Alia,Abdelfatah Aref tmimi and Omaima n.A.AL-Allaf.
[6]. "A high performance fingerprint matching system for large dtabase based on GPU" by PabloDavid,MiguelLastra,Franciscoherrera and Jose Manuel Benitez