ISSN 2277-3061

Three Factor Authentication using Webcam for securing Online Transaction

Vaishali Hirlekar

Assistant Professor, Computer Engineering Department SAKEC, Chembur, Mumbai, India

vaishali.hirlekar@gmail.com

ABSTRACT

There are a continuously growing number of customers who use Online Transaction facility due to its convenience. But the security and privacy of Information may be one of the biggest concerns to the users. In face of the current security issues and the growing number of attacks and consequent frauds, new systems should be designed as to provide better authentication and identification methods. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. A well designed three-factor authentication protocol authentication system can greatly improve the information assurance at low cost. In three-factor authentication, in addition to furnishing their regular password and an OTP, users will be asked to provide biometric information would irrefutably prove their identity. This fingerprint biometric information can be captured by using low cost sensors such as Web Cam. In this paper, we investigate new technique to suitably process camera images of fingertips in order to produce image which are as similar as possible to the ones coming from dedicated sensors. The proposed technique encompasses a segmentation, enhancement and matching of the fingertip image for the person's identifiaction.

Keywords

One Time Password (OTP); Fingerprint Authentication; Region Of Interest (ROI); Segmentation; Feature Extraction.

Academic Discipline And Sub-Disciplines

Computer Science – Data Security and Image Processing

SUBJECT CLASSIFICATION

Image Processing

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol. 14, No. 2

www.ijctonline.com , editorijctonline@gmail.com

ISSN 2277-3061

INTRODUCTION

Today's world is one with increasing online access to services. One part of this which is growing rapidly is conducting financial transactions on a secure website. This system mainly focused on providing online transaction services to customers using web with highly secured technology. So far two factor authentication (2FA) techniques have grown rapidly with enterprises rushing to secure assets in the wake of cyber attacks, compromises and heists. 2FA based one-time password (OTP) techniques along with Smart Card uses basic unique individual identification factors for authentication have done much to secure end-users. However, 2FA authentication technique could also fail if both authentication factors are comprised such as an attacker has successfully obtained the password and the data in the smart card or OTP from users mobile. In that scenario, a three factor authentication (3FA) incorporates the advantages of the authentication based on password, smart card and biometrics. The possibility to obtain biometric information using low cost sensors has a great practical importance. The diffusion of general purpose cameras is rapidly growing and they can found easily on laptops and cellular phones. In this method, once the input image is acquired by the low-cost camera, a preprocessing, feature extraction and matching is done. This entire system authentication significantly improves the information assurance at low cost and also protects client privacy in online transaction system.

RELATED WORK

Fingerprint recognition system is a biometric system that uses fingerprint as biometric input to this system. This biometric system is a computer vision system which performs following functions: Image acquisition, Pre-processing, Feature Extraction, High-level processing or verification or matching. Basically, Fingerprint recognition system is an identification system that can be an Automated Fingerprint Identification System (AFIS). Live-scan acquisition technique is used in civil and criminal AFIS that make use of sensors like optical, solid-state to acquire fingerprints. However, possibility to obtain biometric information using low cost sensors has a great practical importance. The diffusion of general purpose cameras is rapidly growing and they can found easily on laptops and cellular phones. These low cost sensors can be used to capture an image and process the image in such a way that system will produce the result as good as of the dedicated sensors.

In the literature, there are only few works on the usage of low-cost sensor, mainly focused on ridge structure extraction phases. [2] In this paper, once the input image is acquired a pre-processing operation is performed in order to reduce the blue effect. In addition, a of the rid-filtering operation of background subtraction is executed. In parallel, the segmentation of the fingertip region is performed to identify ROI. At post-processing of the ridge structure image is performed by taking into the account the estimation of the local orientation of the ridges. [3] In this paper, texture localization and segmentation is performed initially. A Sobel edge detector is first used to obtain the edge map and localize the finger boundaries. The finger texture image is subjected to median filtering to eliminate the impulsive noise then un-sharpening is done by subtracting a Gaussian filtered image from the original image. The low resolution finger texture images illustrate line like structures and curves, which suggest the feature extraction approaches that can efficiently extract such localized information. Hence, Localized Radon Transform (LRT) and the Gabor-filter-based extraction approaches has been used to achieve high translation and rotational variations.

PROPOSED SYSTEM

3FA SYSTEM MODEL

A well designed three–factor authentication protocol can greatly improve the information assurance. A three-factor authentication protocol involves a Registered User (RU) and a server (S), with biometric characteristics as an additional authentication factor [1]. Three factor authentications consist of three basic phases:-

Phase 1: 3 Factor-Initialization

S generates two system parameters PK and SK. PK is the password shared with the registered user of the system, and SK is kept secret by S. An execution of this algorithm is denoted by 3-Factor-Initialization (k) → (PK, SK), where k is system's security parameter.

Phase 2: 3 Factor-Registration

A Registered User (RU), with an initial password PW and biometric characteristics Bio Data, registers on the system by running this interactive protocol with the server S. An execution of this protocol is denoted by :

RU [PW, BioData] S[SK] $\xleftrightarrow{3-Factor-Reg}$ S[SK]

Phase 3: 3 Factor-Login-Authorization

3-Factor-Login-Auth: This is another interactive protocol between the Registered User (R_U) and the server S, which enables the client to login successfully using PW, OTP, and Bio Data. An execution of this protocol is denoted by

R_U [PW, OTP, BioData] $\xleftrightarrow{3-Factor-Login-Auth}$ S[SK] → {1,0}

The output of this protocol is "1" (if the authentication is successful) or "0" (otherwise).

ISSN 2277-3061

Block Diagram of 3FA system

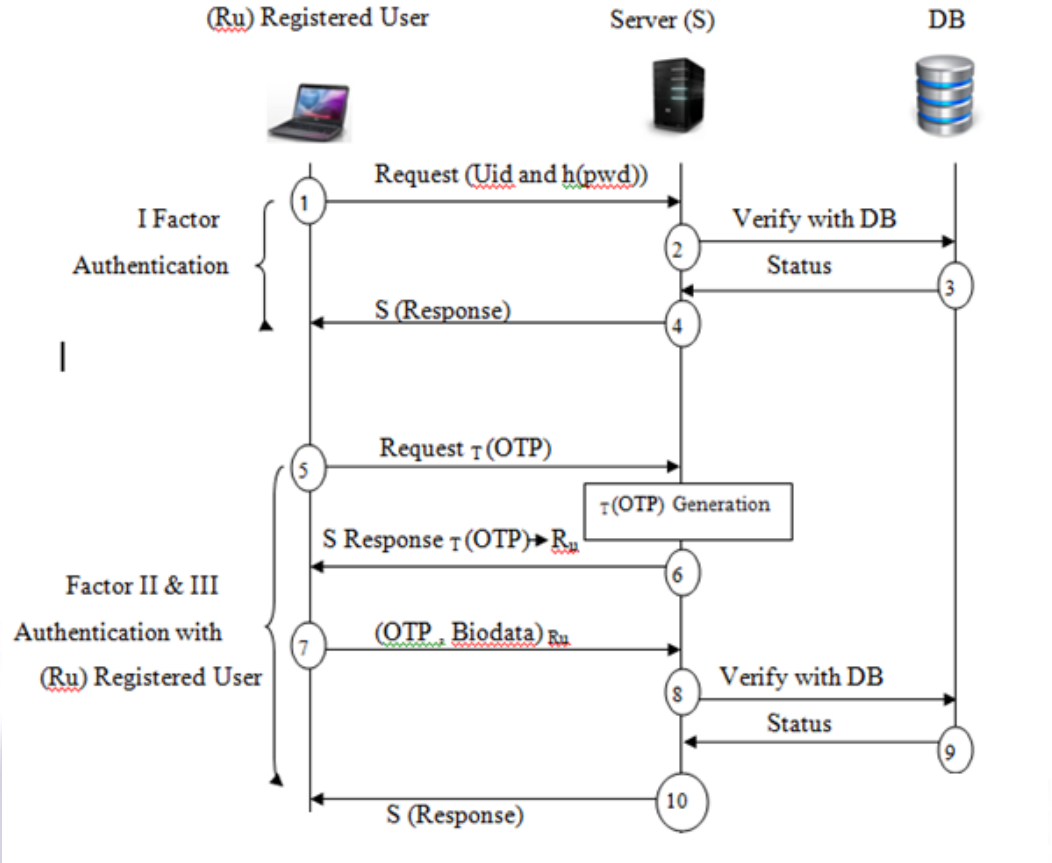

Fig 1: Block diagram of proposed 3FA system

A. Password Encryption Module

In this module, Bcrypt an adaptive Hash function is used specifically for password storage. It uses a modified version of Blowfish Encryption Algorithm. It is used to irreversibly obscure password, just as hash function are used to do a One-way Hash. When a user provides a password that hashes to the value stored in the password table, the registered user will be authenticated.

B. One Time Password Generation Module

TOTP based algorithm is used to generate one time password for the transaction. Time-based One-time Password Algorithm (TOTP) is an algorithm that computes a one-time password from a shared secret key and the current time. TOTP is a hash-based message authentication code (HMAC). It combines a secret key with the current timestamp using a cryptographic hash function to generate a one-time password.

C. Bio-metric Authorization Module

Although this paper is discussing about Three Factor Authentication (3FA) system, more focus is given on Biometric Authentication Module. Wherein fingerprint biometric information can be captured by using low cost sensors such as Web Cam and used further for the user identification and verification purpose.

Fingerprint Biometric as Third Factor in 3FA System

In fingerprint acquisition with Webcam, work is mainly focused on the ridge structure extraction since the contrast between the ridges and the valleys in fingerprint images obtained with a digital camera is low. Second, the depth of the field of the camera is small, thus some part of the fingerprint regions are in focus and some parts are out of focus. Third, the problem of motion blurriness in the acquired images. Thus, the main objective is to find solutions so as to overcome these drawbacks by putting main concern on the fingerprint image pre-processing [2].

The Webcam based fingerprint acquisition system can be divided into three main modules and each module itself consists of some blocks. Each block of a module performs a special function over the input image. The three main sub-division or modules: Pre-processing, Feature Extraction and verification or Matching. The block diagram of the fingerprint recognition system is shown in figure 2.

ISSN 2277-3061

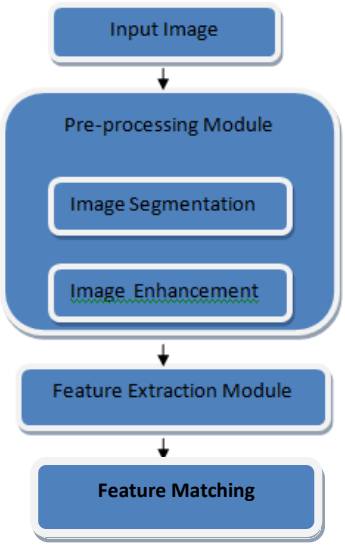

Fig 2: Block Diagram of Fingerprint Recognition System

Proposed Algorithm for Fingerprint Authentication

Pre-Processing Module

Step 1: Read an Input Image

Step 2: Resizing and Gray Scale Conversion

Step 3: Perform Edge Detection

Step 4: Identify ROI based on Edge Detection

Step 5: Binarization

Step 6: Adjust threshold values to find ridge structure.

Feature Extraction & Matching

Step 1: Resizing Ridge enhanced image.

Step 2 :Apply morphological operator to find thinned image.

Step 3: Perform minutiae extraction to find Ridge end and Bifurcation Details.

Step 4: Find x-y coordinate for Ridge end and Bifurcation Feature.

Step 5: Find the match score.

Proposed Method for Biometric Authentication

Pre-Processing

Pre-processing is an important step prior to fingerprint feature extraction and matching. As the fingerprint images are captured using digital camera which had certain challenging problems as stated earlier so, these fingerprints require more pre-processing over them. Pre-processing is divided into four blocks.

a. Gray Scale Conversion

The fingerprint images captured by using digital camera are in RGB format, so RGB to greyscale image conversion is done. A greyscale image has 256 different gray levels which are sufficient for the recognition of most natural objects .In a gray-level fingerprint image, ridges and valleys in a local neighbourhood form a sinusoidal-shaped plane wave which has a well-defined frequency and orientation.

b. Segmentation

Segmentation of fingerprint image is necessary so as to reduce the size of the input data, to eliminate undesired background which is the noisy and to focus on area which is in favor of the central part of the fingerprint.

c. Region of interest

A region of Interest is a portion of an image that to be filtered or can be used to perform futher operation on it. Region of Interest is determined here based on the edge detection of an Image. After the region of interest is determined, the image is threshold into a binary image with adaptive thresholding.

d. Binarization

Image Binarization is a process which transforms the 8-bit Gray image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image. In this method image is divided into blocks of pixels. A pixel value is then set to 1 if its value is larger than the mean intensity value of the current block to which the pixel belongs.

e. Ridge Enhancement

Ridge enhancement is done in case of some ridges are hidden or not visible because of low intensity then in that case first zooming of that region is done in order to increase the size of the area that will give more focus on the gaps and give better result of ridge structure.

Feature Extraction and Matching

a. Minutiae Extraction

A fingerprint is composed of ridges and furrows which are very similar to the other fingerprints. However, minutiae are the abnormal points on ridges and furrows. Among all the fingerprint features, the minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem. Minutiae are the finest local features which differ from fingerprint to fingerprint. Minutiae points are detected by locating the end points and bifurcation points on the thinned ridge skeleton based on the number of neighbouring pixels. Now that we have enhanced the image and segmented the required area, the job of minutiae extraction closes down to three operations: Ridge Thinning, Minutiae Marking and Minutiae Representation.

Ridge Thinning

In this process we eliminate the redundant pixels of ridges till the ridges are just one pixel wide. This is done using the MATLAB's built in morphological thinning function.

Minutiae Marking

Minutiae marking is now done using templates for each 3 x 3 pixel window. If the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only one-value neighbors, then the central pixel is a ridge end.

Minutiae Representation

Finally after extracting valid minutia points from the fingerprint they need to be stored in some form of representation common for both ridge ending and bifurcation. So each minutia is completely characterized by the following parameters 1) Bifurcation_x-coordinate, 2) Bifurcation_y-coordinate, 3) Ridge_x-coordinate 4) Ridge_y-coordinates

b. Matching

Minutiae based matching is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings.

REQUIREMENT ANALYSIS

Fingertip Registration Phase

Fingertip registration operation is required to scale and rotate the fingertip image so that the input image is transformed in a standard image should have the following characteristics:

a. Center of the fingertip should be placed at the center of the image.

b. Orientation of the fingertip should be horizontal.

c. The fingertip image should be captured from the proper distance.

However, note that the use of webcam as a biometric sensor produces significant variations of scale, position and rotation of the fingertip at different time of image acquisition.

EXPERIMENTAL RESULTS

Experiments has been carried out by using a webcam (iBall Face2Face Webcam at 640X480 pixels) and by capturing 50 different live images. Figure shows the experimental results as below.

ISSN 2277-3061

Fig. 3a Input Image

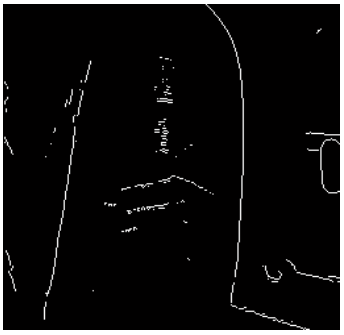

Fig 3b Edge Detection

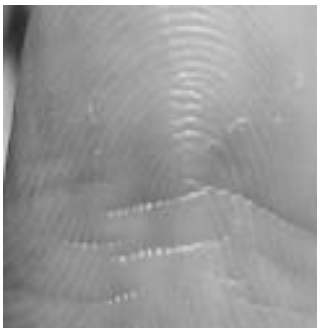

Fig. 3c Segmented Image

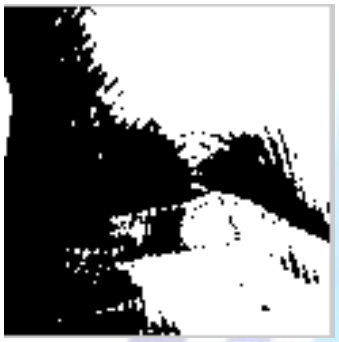

Fig. 3d Binarized Image

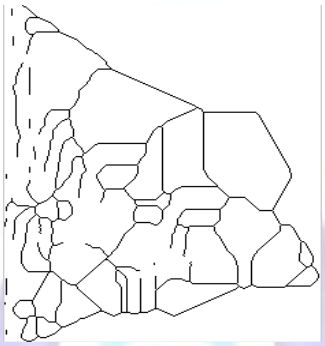

Fig. 3e Ridge Thinning

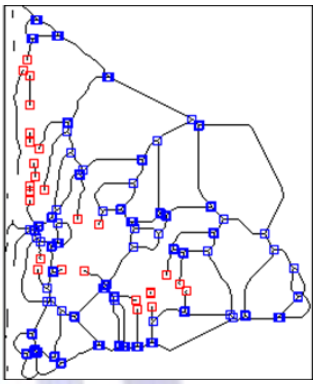

Fig. 3f minutiae points

Minutiae Matching

At the matching stage, approach is to elastically match minutiae. Given two set of minutia of two fingerprint images, the minutiae matching algorithm determines whether the two minutia sets are from the same finger or not.

Table 1 shows False Acceptance Rate (FAR) , False Rejection Rate (FRR)

False Acceptance Rate	0.24
False Rejection Rate	0.222

CONCLUSION

This paper presented an innovative composition of technique to extract the fingerprint ridge structure and use as a third factor to provide better authentication and identification method. Since the characteristics of fingerprint images acquired with a webcam are quite different from those acquired by conventional touch-based sensors, a new fingerprint pre-processing algorithm was used. The main contributions of this paper are pre-processing techniques that can be executed for fingerprint image enhancement,feature extraction and matching. We have found that this clearly outperforms defining the features from a very low quality fingerprint captured by a low priced webcam.

An entire approach we propose aims to provide a well designed three-factor authentication protocol authentication system can greatly improve the information assurance at low cost. Additionally using low cost camera as interoperable device in the online transaction system increases the feasibility, availability and ease of the system.

REFERENCES

[1] Xinyi Huang, Yang Xiang, Member, IEEE, Ashley Chonka, Jianying Zhou, and Robert H. Deng, “A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems”, IEEE transactions on parallel and distributed systems, vol. 22, no. 8, august 2011.

[2] Vincenzo Piuri, Fabio Scotti, “Fingerprint Biometrics via Low-cost Sensors and Webcams”, IEEE, 2008.

[3] Ajay Kumar, Senior Member, IEEE, and Yingbo Zhou, “Human Identification Using Finger Images”, IEEE transactions on Image Processing, vol.21, no. 4, April 2012.

[4] Ravi, H. ; Sivanath, S.K. Technologies for Homeland Security (HST) ,"A novel method for touch-less finger print authentication", IEEE International Conference, 2013.

[5] Syeda Farha Shazmeen, Shyam Prasad, "A Practical Approach for Secure Internet Banking based on Cryptography", International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012.

[6] Maneesh Upmanyu, Anoop M. Namboodiri, K. Srinathan and C.V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010.

[7] Petr Hanaeek, Kamil Malinka & Jiri Schafer, " e-Banking Security - A Comparative Study", IEEEA & ESYSTEMS MAGAZINE, 2010.

[8] Behrouz A. Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 2nd Edition.

[9] Nina Godbole, Sunit Belapure, "Cyber Security", W1ley India, New Delhi.

[10] Rolf Oppliger , Ruedi Rytz, Thomas Holderegger, "Internet Banking: Client-Side Attacks and Protection Mechanisms" in IEEE Computer Society, 2009.

[11] Thomas Weigold, ThorstenKramp, and Michael Baentsch, ""Remote Client Authentication" in IEEE Computer Society, 2008.

[12] Alain Hiltgen, Thorsten Kramp and Thomas Weigold, "Secure Internet Banking Authentication" in IEEE Computer Society, 2005

Author' biography with Photo

Vaishali Hirlekar recived the (A.M.I.E.) in Computer Science and Engineering from Institution of Engineers (India) and persuing ME in Computer Engineering from Mumbai University.