International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

FASSBTR: Fingerprint Authentication System Security Using Barcode and Template Revamping

Anik Lal T. S[1]

[1]*PG Scholar, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thiruvilamala, Kerala, India*

Abstract - *At present, a drastic change has been developed in the count of consumer electronic gadgets: such as Locking systems, Smartphones. These devices are subsumed with fingerprint sensors for authorised personnel authentication. The sensors integrated in these devices are generally small and the resulting images are therefore limited in size for the purpose of portability . This paper scrutinizes the security login layer and incorporates the fingerprint enhancement level of histogram equalization and revamping the templates of the partial fingerprint-based authentication systems. Here in this paper, Firstly the user must enter their credentials in order to move onto their fingerprint authentication process. It takes only two revamped fingerprint impressions of a single user while enrolling.*

Key Words: **Authorised, Enrolling, Revamp, Partial, Templates**

1. INTRODUCTION

At present, there are several vulnerabilities like Fingerprint spoofing, Fingerprint remoulding and low built quality of the small sized sensor used in the fingerprint based authentication system. To compensate the issue of mini sized sensors, these devices acquire exactly two partial impressions of a single finger during enrollment as a part of security, to ensure that only one of the exact revamped impression will match successfully with the image obtained from the user during authentication.

A user is said to be successfully authenticated if and only if the security login layer is passed, then only the fingerprint authentication process starts and obtain impressions via enrollment otherwise if false credentials is placed the complete process closes. During verification it must exactly match one of the stored templates. Here it produces a multiple layer security that is difficult for an attacker to break. Some of the most common finger spoofing methods and types of fingerprint scanners are mentioned below.

2. PRIOR WORK

The prior work focuses on the templates that are mainly obtained from the partial fingerprints rather than full prints via calculating the number of minutiae points. There are three major research topics in the Prior work that are highly connected to the proposed work and they are :Wolf Attack Probability (WAP), Masterprint, Evidential Value Analysis.

2.1 Masterprint Generation and Existence

Hypothesis

The print generation and existence hypothesis process is tested by performing the experiments that were conducted on the FVC 2002 dataset that contains 8 prints of 100 subjects, for a total of 800 prints. Created partial prints of size (w x h) by cropping the full prints using an overlapping window that moved from top-bottom and left-right with a half percent overlap between adjacent windows.

Two approaches: First, where the print is selected from an existing dataset of real fingerprints. Two, where the print is generated synthetically. SAMP: MasterPrints by sampling a fingerprint dataset The "Imposter Match Rate" (IMR) - which is the count of false matches when a fingerprint is related against templates of other fingers (impostors) is computed for all candidate prints. SYMP : Generate improved MasterPrints synthetically by maximizing their IMR over the dataset. The prints with maximum IMRs are selected from the dataset.

2.2 Wolf Attack Probability

[2] proposed a security measure called "WAP", it estimates the strength of a biometric authentication system against impersonation attacks. In this work, a wolf is defined as any input sample, including non-biometric samples such as physical artefacts, that can falsely match with multiple biometric templates.

2.3 Evidential Value Analysis

A.Nagar [3] proposed, a framework developed to acquire the evidence of a given fingerprint match score in terms of nonmatch probability (NMP), namely, the posterior probability that the pair of fingerprints being compared are not match. The change in NMP values linked with the fingerprint databases having specific print characteristics (image quality, size and minutiae count).

The NMP values acquired from different partitions of a fingerprint database are compared using a measure, named the conclusiveness that computes the significance of evidence associated with an NMP value. Due to paucity of a large set of latent prints, rely and focus on the partial prints obtained by cropping exemplar prints to simulate latent prints and reveal the effectiveness of this simulation.

2.4 Computation of Indirect Attacks and Countermeasures in Verification Systems

M. Martinez-Diaz [4] proposed and analysed the Biometric recognition systems are extremely vulnerable to several security threats. These includes direct attacks or indirect attacks to the sensor, which indicates the one aimed towards the interior system modules. Indirect attacks against fingerprint verification systems are analyzed in order to calculate how harmful they are. Software based attacks via hill climbing algorithms are implemented and their success rate is observed under several conditions.

Hill climbing attacks are generally highly effective in the process of developing synthetic templates that are accepted by the matcher as genuine. Score quantization has been learnt as a needful counter-measure against hill climbing attacks.

2.5 Effect of Artificial Fingers on Fingerprint Systems

T. Matsumoto [5] Proposed that Artificial fingers causes major potential threats to the system. Dummy fingers are very complex for the authentication process on the fingerprint systems. Computation against attacks using such artificial fingers has been disclosed very rarely. The acceptance count range of live fingers is greater than that of gummy fingers for some systems that may be named as live and Ill detection. If "live and Ill" detectors can clearly distinguish their moisture, electric resistance, transparency or bubble content then the fingerprint systems can reject gummy fingers. Detection of compliance is a major part for preventing gummy fingers.

2.6 Antispoofing Schemes for Fingerprint Recognition Systems

E. Marasco [6] Proposed a technical study based on the vulnerability of the fingerprint recognition system and counter-attacks have been noted in detail in this literature. One such vulnerability involves the use of artificial fingers, where materials such as Play-Doh, silicone, and gelatin are inscribed with the ridges. The main sections of Antispoofing schemes are Hardware and Software based.

2.7 Fingerprint Template Selection

U. Uludag [7] Proposed a Fingerprint authentication system operates by acquiring a fingerprint data from a user and running the similarity measure against the template data stored in a database in order to identify a person or to verify a claimed identity. Many authentication systems store multiple templates per user in order to collect variations analysed in a person biometric data. In this section there are two methods to perform template selection automatically where the main aim is to select the feature or core point of the fingerprint templates for a finger from a given set of fingerprint impressions. The first method, named DEND, initializes a grouping concept to choose a template set that represents the best intra-class micro changes, while the second method, called MDIST, chooses the templates that exhibit maximum similarity with the remaining impressions.

2.8 Presentation Attack Detection Methods

C. Sousedik [8] Proposed that Fingerprint biometrics is used in various gadgets, to control the access towards the security based environments. Any fingerprint system is highly vulnerable against a fake fingerprint characteristic. Fingerprint systems spoofing is one of the most widely researched areas. The top rated sensors can also be duplicated by an accurate imitation of the ridge or pores structure of a fingerprint. An individual registered user avoid identification by altering his own fingerprint pattern.

The efficiency of the methods strongly depends on the knowledge of the artificial fabrication techniques and quality of the materials used during the development of the method. The fake fingerprints are used to spoof the sensor, therefore the standard dataset are used and it should contain a large number of scans captured by using high-quality fake fingerprints.

2.9 A technical evaluation of fingerprint scanner

[9] A major technical parameter with high importance is the resolution section, that is the number of pixels per inch (**dpi**) characterizing the acquired images. According to the base architecture of the scanner system, the scanner with high resolution produces the finer detailing that can be extracted from a fingerprint image. A 500 dpi resolution is required by higher officials or agencies for their processing.

Another major section is the size of the scanner sensing area, this parameter focuses the size of the fingerprint portion which can be acquired by the scanner. The small overlapping area between fingerprint acquired at different times is one of the main causes of false rejections (FRR) in fingerprint systems.

2.10 Barcode System Technology

In [10] this section we take the concept of Barcode-128 symbology, It is one of the most modern and high density barcode system which helps in storing ASCII codes as well as alphanumeric values. It uses a built-in check digits, It is a part of the code and cannot be omitted. It is not mentioned in human readable format.

3. MODUS OPERANDI

This paper proposes the timer-based user credentials login layer and enhancing the template by applying the cumulative histogram equalization and revamping the fingerprint image for reprocessing the lost minutiae points which helps in raising the accuracy of the partial fingerprint recognition.

3.1 User Credentials Login Layer

The main goal of this layer is to protect the privacy of the user from unauthorised personnel's. The steps are mentioned below

STEPS:

1. The authorised users will be provided with the QR/ Barcode code consists of their own passcode and user-id which is developed with combination of numbers and alphabets with 15 digits based on their device model frame code.

2. The particular QR / Barcode can only be accessed by specified readers which is another security highlighted in this layer.

3. The major section is, if the user-id or passcode is typed wrong the whole session closes and without passing this layer the fingerprint authentication section will not be accessible.

3.2 Histogram Equalization Algorithm

In this paper, Partial Fingerprint is enhanced by increasing the contrast of the input template using the histogram equalization algorithm and a new furnished image is developed accordingly.

STEPS:

1. The value of occurrences is calculated using the gray scale level *k*. Where *K* represents the total number of gray levels in the image.

2. The probability of an occurrence of a pixel of level *k* in the image is calculated.

3. The Corresponding Cumulative distribution function is calculated.

4. A transformation of the form $k' = T(k)$ is created to produce a new image.

5. New image is calculated according to k' value. Collect the new image and its Histogram.

3.3 Fingerprint Revamping Using Filters

Here In this paper, the degraded fingerprints with cuts and scars are collected and processed to redevelop the partial fingerprint templates.

STEPS:

1. The low quality partial fingerprints with cuts and scars or with lost miutiae points are chosen.

2. The chosen template is converted to grey image inorder to remove the false contents of the image background.

3. Then segmentaion of the template is performed by normalising and segmenting the ridge region.

4. Then estimates the local orientation of the ridges in a template by calculating the image gradients and plotting the values.

5. To estimate the fingerprint ridge frequency by considering blocks of the image and % determining a ridge count within each block.

6. Finally we get the image with fillings in the missing areas in a binarized form.

3.4 Partial Fingerprint Feature Unsheathing Levels

1) Image Acquisition

This section controls the handling of the images that are ready for processing.

2) Image preprocessing

Here in this section there are two operations to be performed as a main they are: Binarization, Segmentaion.

Binarization : It is the process of transforming image to black and white form of pixels within a specified threshold value. Here the 8 bit value is converted to 1 bit value with furrows represented as '1' and ridge as '0' value.

Segmentation: In this layer the background and foreground is divided using the block wise threshold variance inorder to place a sharper image.

3) Ridge Thinning

It is a technique which is mainly forwarded to eliminate the excess pixels of ridges till it reaches 1 pixel width. It is mainly performed via morphological process. It produces a high contrast and sharpness to the template image.

4) Locating Minutia Points

It is mainly processed in order to collect the minute points of the fingerprint template . It uses the concept of Crossing Number. These minutiae points are exactly collected using the Neighborhood operation on each ridge pixel of the image using 3 x 3 window. The neighbouring section with only value 1 is taken as ridge ending.

5) Region Of Interest

In this process the bounded region of the closing area is subtracted from the opening area accordingly where the algorithm makes the selected area tightly by eliminating the rest of the areas.

6) Eliminating False Minutia

This layer does not completely recover the image, but it removes the excess points with darker content which is fake or overlaped due to high pressure application on the sensor.

3.5 AUTHENTICATION SYSTEM

In this paper Authentication system consists of two modules they are as mentioned below:

Enrollment: Here the authorised user places two impressions for enolling to the database for further purposes. As a part of security only two impressions are taken in and stored to the database since it is very complex to get a similar impression after applying revamping layer.

Verification: It is the section where the data that is given as an input is checked with the files in the database which is having high similarity value when related with the mentioned threshold value.

3.6 DATABASE MATCHING USING FVC2002 AND VERIFINGER SDK 1.6

Database matching is the process of comparison between two files or more to check whether any similarity measure is taking place for exact matching file to obtain and it is mainly based on the mentioned threshold value.

Using FVC2002:

One To Single Check : Process of taking the input image and comparing it with the image that is already stored in the database to get a similarity meausre level.(One to One)

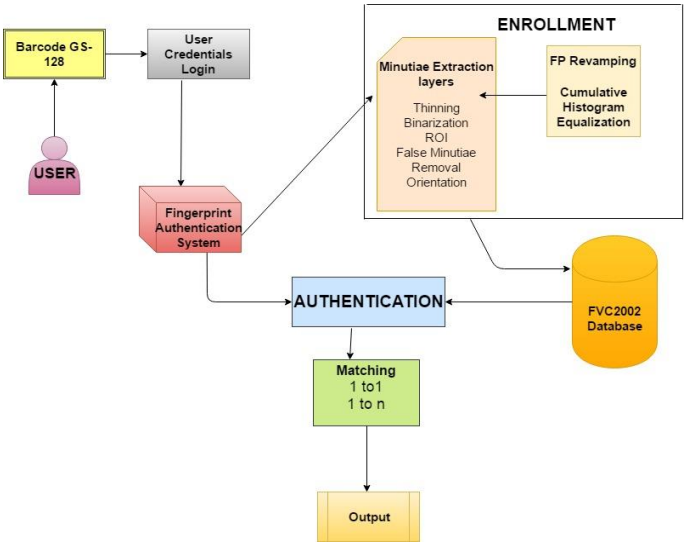
One to Many Check: Process of taking the input image and comparing it with whole database in order to obtain the complete list of matches.

Using Verifinger SDK 1.6: In this section the SDK uses the input image to compare it with the whole data in the database for crosschecking the image in detailed. It is more faster and sharper, more accuracy is shown using this sdk process.

Table - 1: Analysis of Fingerprint

Types Of Fingerprint	Acceptability	Universality	Performance
Live fingerprint	HIGH	MEDIUM	HIGH
Degraded live print	HIGH	LOW	MEDIUM
Synthetic Print	LOW	MEDIUM	LOW

3.7 SYSTEM ARCHITECTURE



4. RESULTS AND DISCUSSION

According to the performance evaluation of partial fingerprints authentication system, using the concept of User Credentials locking layer and Fingerprint Enhancement layers like : Histogram Cumulative Equalization and Kovesi Revamping (Reconstruction)there occurs a slight variation in the rate. Here FVC 2002 DB-1(B) is used as the database for computing.

Table-2 shows the Efficiency rate without the User Credentials Layer and Fingerprint Enhancement Layers, The next table shows the Efficiency rate with the User Credentials Layer and Fingerprint Enhancement Layers marked as Table-3. When evaluating at core level Table-3 shows the better improvement in the accuracy and efficiency level when compared with Table-2.

Table-2: Efficiency and Accuracy test rates based on the types of Fingerprint without Security Layer and Enhancement Layer

Fingerprint Types	No. of Templates Dataset	Correct Prediction (in %)	Wrong Prediction (in %)
Live Finger	80	37.5%	32.5%
Degraded Live Finger	80	30%	25%
Synthetic Finger	80	22.5%	17.5%

Table-3: Efficiency and Accuracy test rates based on the types of Fingerprint with Security Layer and Enhancement Layer

Fingerprint Types	No. of Templates Dataset	Correct Prediction (in %)	Wrong Prediction (in %)
Live Finger	80	47.5%	40%
Degraded Live Finger	80	37.5%	27.5%
Synthetic Finger	80	20%	10%

5. CONCLUSION

In this paper, the proposed system includes the concept of User Credentials login system via barcode for privacy and incorporated the fingerprint system with histogram equalization to enhance the image even after application there are several flaws in the templates. For further perfection added the concept of Fingerprint Revamping, which shows the performance rise in the authentication system and rejects fake users access.

REFERENCES

[1] Arun Ross, Nasir Memon, Aditi Roy. "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems", IEEE Transactions on Information Forensics and Security, DOI 10.1109/TIFS.2017.2691658

[2] M. Une, A. Otsuka, and H. Imai. Wolf attack probability: A new security measure in biometric authentication systems. In International Conference on Biometrics, pages 396–406. Springer, 2007.

[3] A. Nagar, H. Choi, and A. K. Jain. Evidential value of automated latent fingerprint comparison: an empirical approach. IEEE Transactions on Information Forensics and Security, 7(6):1752–1765, 2012.

[4] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognition Letters, 32(12):1643–1651, 2011.

[5] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In Electronic Imaging, pages 275–289. International Society for Optics and Photonics, 2002.

[6] E. Marasco and A. Ross. A survey on antispoofing schemes for fingerprint recognition systems. ACM Computing Surveys (CSUR), 47(2):28, 2015.

[7] U. Uludag, A. Ross, and A. Jain. Biometric template selection and update: a case study in fingerprints. Pattern Recognition, 37(7):1533– 1542, 2004.

[8] C. Sousedik and C. Busch. Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biometrics, 3(4):219 – 233,2014.

[9] A technical evaluation of fingerprint scanners. http://www.biometrika.it/eng/wp scfing.html. Accessed Jan. 2016.

[10] TEC-IT Barcode System, http:// www.tec-it.com, TEC-IT Datenverarbeitung GmbH, Hans-Wagner-Str. 6, A-4400 Steyr, Austria.