SURVEY ON FINGER PRINT RECOGNITION SYSTEMS FOR IMPROVED CLOUD SECURITY

Dr. N. Venakatesan
Department of Information Technology,
Bharathiyar College of Engineering Technology, Karaikal, India

M. Rathan Kumar
Research Scholar, PRIST University, Thanjavur, India

ABSTRACT

Biometrics is a rapidly evolving technology and is being widely used in authentication systems in today’s networked world. In an era, where the hardware and software services are available on cloud, the application of biometrics has increased a lot. The availability of inexpensive hardware devices like fingerprint scanner in mobile phones have also contributed a lot in biometrics authentication systems. Fingerprint authentication is possibly the most sophisticated method of all biometric techniques and has been thoroughly verified through various applications. Even features such as persons gait, face or signature may change with passage of time and may be fabricated or imitated. However a fingerprint is completely unique to an individual and stayed unchanged for lifetime. This paper discusses the various aspects and methods to be applied for the fingerprint-based identification system.

Key word: image processing, bio-metric images, fingerprint recognition, authentication.

Cite this Article: Dr. N. Venakatesan and M. Rathan Kumar, Survey on Finger Print Recognition Systems for Improved Cloud Security. International Journal of Computer Engineering & Technology, 8(5), 2017, pp. 78–86.

1. INTRODUCTION

This research paper concentrates mainly on bio-metric image processing techniques and tries to evolve an approach on how to incorporate the security features in cloud using the bio-metric image processing techniques. The definition for Bio-Metrics as per [1], ‘Bio-Metric Technologies are automated methods of verifying or recognizing the identity of a living person on a physiological or behavioural characteristic’. The keyword “automated methods” conveys us a lot: the authentication is done by a machine, may be a computer not necessarily to be a computer.
Then we look upon another important keyword “person” that needs to be thoroughly analysed and understood. The physiological and behavioural characteristics of people vary definitely, if the take into account: DNA, hair, finger print, iris image, body odour etc. The simple id/pwd mechanism for security has become more trivial to hack; hence identifying the correct user to access the cloud resources by using biometrics-based authentication over other authentication methods, is being widely practiced and there has been a significant increase in the use of biometrics for user authentication in recent years, in the banking, financial services and insurance sectors.

The importance of biometrics-based authentication systems that are designed to withstand security issues when employed in critical applications, especially in independent remote applications such as e-commerce, banking is to be clearly addressed. Our focus is towards using such bio-metric authentication systems in cloud environment where an enterprise’s business data is stored in remote servers.

In this paper we discuss few of the bio-metric based authentication systems, especially finger print based authentication and also identify the serious issues in systems implementing biometrics-based authentication, and present improved methods to overcome of these security issues, when private data is ported to a public cloud.

2. RELATED WORK
2.1. The Need for Bio-metrics
The relationship between man and man has reduced and the relationship between man and machine has increased. The digital divide is narrowing down. While talking about the conversation between man and machine, the process of identification arises. When we use machines in public environment say the cloud, and then identification of the user is very much necessary. The thin gap between man and machine is reduced using various methods and bio-metrics authentication is also one important technology amongst them. The various bio-metric techniques used in the present day are: face, fingerprint, iris image, voice recognition, hand geometry, retinal pattern, signature, thermo-grams etc.[2]

Some bio-metric techniques are still in pipeline viz. odor, ear, keystroke, DNA, hair. In our paper, fingerprint authentication mechanism is analyzed and the way to incorporate such authentication mechanism in a cloud environment to provide secured services to the data owner is discussed.

3. RECOGNITION TECHNIQUES
3.1. Finger-Print Identification – Technique 1
The process of identification in this networked world is inevitable. When we use web services like mail, banking, ecommerce, and for the present day, when we use cloud, we have identification mechanisms like user-id, password, one time pin etc. Identification process [2] can be well understood as: ‘something you possess’ and ‘something you know’. An example scenario is: we possess ATM card and we know its PIN number. What if we lose our ATM card and most of the users have their PIN as year of birth kind of data. If an imposter possesses our ATM and has our PIN, then the identification process fails.

In order to improve this vulnerable identification process, we use bio-metrics to strengthen the identification process in this networked world. What could be taken as bio-metric identification? The answer is any human physiological or behavioral characteristic could be accounted as a bio-metric identification provided that satisfies few properties as
detailed: i) universality – all human should possess, ii) uniqueness – no two humans have the same, iii) permanence – should not vary with time and iv) collectability - quantifiable.
The bio-metric based authentication is widely used in many of the applications: banking, e-commerce and now in cloud environment too to ensure security of data in storage as well during communication.

3.2. Finger Print - Authentication
Fingerprints are unique amongst individuals. In the field of Astrological Science, fingerprints provide vital information to predict about future life of an individual. Finger prints are graphical flow-like ridges in palm of a human. Finger print is captured digitally using a finger print scanner, such hardware components are being incorporated in the present day mobile phones. Hence adding biometrics security to the cloud infrastructure will not be a problem for the present day as its hardware counterpart is less expensive and can also be easily interfaced with the existing system.

Ridge ending and ridge bifurcation are the two important characteristic features in finger print of any human user. A common algorithm has been developed and widely used: “automatic fingerprint identification system” that consists of two steps: off-line and on-line. In the off-line phase, a fingerprint is captured using the hardware device, and the captured image’s quality is improved using different algorithms; then significant features of the fingerprint are extracted and stored in a database as a template. In the on-line phase, the fingerprint of the user is captured, enhanced and features of the fingerprint are extracted, and is compared with the template stored in the database during on-line phase. The steps are illustrated in the figure 1.

Though we have many other biometric solutions, fingerprint identification system is widely used for many reasons. Comparing to other biometric techniques, the advantages of fingerprint-based identification are as detailed below: (1) uniqueness of the fingerprint - the minutiae details of individual ridges and furrows are permanent and unchanging. (2) The fingerprint is easily captured using low cost fingerprint scanner. (3) Fingerprint is unique for every person. So it can be used to form multiple levels of security to improve cloud systems.

The figure below clearly explains the simple methodology of fingerprint verification. In off-line process, the fingerprint of all users are captured and stored in a database. Before storing the raw or original image, the image is enhanced. The fingerprint image when captured for the first time may contain unwanted data ie noise. Because our hands being the most used part of our body may contain wetness, dry, oily or grease; and these images may be treated as noise while capturing the original finger print. And hence, to remove the noise, image enhancement techniques like adaptive filtering and adaptive thresholding.

![Figure 1 Flow of Diagram representing the Fingerprint Identification](http://www.iaeme.com/IJCET/index.asp)
The standard form factor for the image size is 0.5 to 1.25 inches square and 500 dots per inch. In the above original image, the process of adaptive filtering and thresholding are carried out. The redundancy of parallel ridges is a useful characteristic in image enhancement process. We can determine the flow by applying adaptive, matched filter even though there may be discontinuities in a particular ridge. This filter is applied to every pixel in the image and the incorrect ridges are removed by applying matched filter. Thereby, the noise is removed and the enhanced image is shown in figure 3.

The enhanced image undergoes feature extraction process wherein: binarization and thinning take place. All fingerprint images do not share same contrast properties as the force applied while pressing may vary for each instance. Hence, the contrast variation is removed by this binarization process using local adaptive thresholding.

When the width of the ridges is reduced down to a single pixel, an improved fingerprint image is obtained and this feature extraction process is called Thinning. The resultant feature extraction is shown below figure 4.

The process of minutiae extraction is done as the last step in feature extraction and then the final image is stored in database. When the image is thinned down, it is very easy to extract the features: the minutiae are straightforward to detect and the endings are found at the termination points of thin lines and the bifurcations are found at the junctions of three lines.
Once we are able to identify valid minutia points in a thinned image, then we have to extract two important data from the enhanced, thinned image based on the significant minutia points: they are ridge ending \((x,y)\) location, and the direction of the ending bifurcation. Although minutia type is usually determined and stored, many fingerprint matching systems do not use this information because discrimination of one from the other is often difficult. The result of the feature extraction stage is what is called a minutia template, as shown in figure 5. This is a list of minutiae with accompanying attribute values. An approximate range on the number of minutiae found at this stage is from 10 to 100. If each minutia is stored with type (1 bit), location (9 bits each for \(x\) and \(y\)), and direction (8 bits), then each will require 27 bits—say 4 bytes—and the template will require up to 400 bytes. It is not uncommon to see template lengths of 1024 bytes.

Now, the online process starts. At the verification stage, the fingerprint of the cloud user who wants to access cloud services is captured and his template is compared with the fingerprint database. Minutiae are grouped based on their proximity and referred as neighborhood minutiae. Rather checking each and every processed minutia with the stored minutia, this grouping of neighborhood minutiae helps in easy and quicker matching process. Usually, three or more minutiae are grouped as one neighborhood minutiae.

![Figure 5 Minutiae Template](image)

Each of the neighborhood minutiae is located at a certain distance and relative orientation from each other. First matching of neighborhood minutiae is carried out between the two images; if similarity is found to a satisfactory threshold, then few neighborhood minutiae are sampled and the individual minutia in the neighborhood minutiae of the users current fingerprint image and the database stored image are compared further. As each minutia has its own attributes of type and minutia direction, individual minutiae are also compared. If comparison indicates only small differences between the neighborhood in the stored fingerprint and that in the current user’s fingerprint, then these neighborhoods are said to match. This process is carried out for all the neighborhood patterns exhaustively and if enough similarities are found, then the fingerprints are said to match. Another method for matching the fingerprint images is called template matching. A graph pattern has to be conceived by interconnecting the minutiae and is compared with the shapes of graphs joining fingerprint minutiae. This is illustrated in Figure 6. A 1:1 matching cannot be carried out and we use a threshold value—termed as match score, usually a number ranging between 0 and 1. Higher the value, higher is the match.
3.3. Finger-Print Identification – Technique 2

Wavelet Packet Correlation Method in Biometrics

Correlation filter is an accurate approach to detect and locate low contrast character strings in complex table environment. It uses shift-Invariance It comparing the proposed wavelet packet filters to standard filters, We see a significant improvement in accuracy.

3.4. Finger-Print Identification – Technique 2

Neurocomputing

Author in [11] introduces LDSSs (long digital straight segments) technique for fingerprint recognition. Each digital straight segment is measured by using the four parameter: x, y coordinate, slope and length. This information needs about 500-600 bytes to store.

As a result, LDDS is a best technology compared to orientation field. For capturing the global structure of the finger-print. This paper shows that the combining the minutiae and LDSSs features gave the better performance as compared to the minutia based method.

3.5. Finger-print Identification – Technique 3

A Hybrid System For Fingerprint Identification

Due to the poor performance of minutiae based method, for real time authentication, author in [10] introduce the hybrid finger-print matching system which combines the minutiae features and wavelet statistical features. In this research fingerprint matching is done by the following method:

- Minutiae based method
- Wavelet transform based method

![Figure 7 Hybrid systems for fingerprint recognition [10]](http://www.iaeme.com/IJCET/index.asp)
The performance of hybrid fingerprint recognition is measured by FRR (False Reject Rate) and FAR (False accept Rate). This method is well suited for real-time authentication system with a number of fingerprint as compared to conventional minutiae based method.

### 3.6. Finger-Print Identification – Technique 4

**Consensus Fingerprint Matching With Genetically Optimized Approach**

Author [4] introduce a new approach in which first suggest a consensus matching function then devise a genetically guided approach to optimize the consensus matching function for simultaneous fingerprint alignment and verification.

The experimental results of proposed algorithm shows that the consensus function can lead to a substantial improvement in performance while the local matching operation helps to identify promising initial alignment configuration, thereby.

Authors in [3] propose two new methods to detect the fingerprints of different persons based on one-dimensional and two-dimensional discrete wavelet transformations (DWTs).

In first method several fingerprints of a person are taken in a random manner followed by a two-dimensional DWT. Four filtered signals (level-one (approximation), level-two (horizontal details), level-three (vertical details), and level-four (diagonal details)) A, B, C and D are again transformed at 9 levels DWT and the approximations are stored instead of the original images. The transformed signal matrices $Ti,n = [Ai,n Bi,n Ci,n Di,n]T$; where n = 1, 2, 3, ..., M, and M is the number of stored matrices of user i. To recognize the fingerprint of a person, his image is scanned and the same job is done to determine the matrix $Ti,n$. Finally, a convolution is made with stored vectors $yi$ of $Ti,n$ and the corresponding vectors of the present scanned image and corresponding convolution vectors $vi$ are stored.

In second method, several fingerprints of a person are taken in a random manner as in the previous method (in context of translation and rotation) then an RGB conversion is performed on them. The contrast of the images is increased using a Canny filter then colour inversion is performed on them. The results section of this paper considers only three fingerprints in the process of finding similarities and dissimilarities. Here, only Canny filter is used for image processing.

Authors in [6] introduce the task of recognizing characters in natural Scenes like clutter and placement, Different font style and Variation in light conditions. Author implemented two common descriptors: shape context and wavelet. In shape context method, extract the relative positions of pixels in an edge image. For each location, we impose a log-polar grid and bin the pixels in the edge image into a histogram. Second Wavelet transforms have been used for texture representation, image compression and character recognition.

We concluded that the recognition performance of shape context is poor while the performance of wavelet is slightly less than the performance of the raw data descriptors.

Authors in [5] used level 2 daubechies transform and only the second level LL image is used for the analysis as that contains most of the important texture information. Daubechies deals with problems associated with JPEG compression and random additive noise. Authors propose a combination of three texture descriptors namely Standard Deviation, Kurtosis and Skewness. DWT is the transform used for analysis. Canberra distance metric is used for similarity estimation. This approach is very simple compared to minutia point pattern matching algorithm. It is robust as DWT is rotation invariant transform.
Present and Future Use of Fingerprint Recognition

Fingerprint recognition system is widely used in forensic applications like criminal investigations, terrorist identification and other security issues. As fingerprint recognition technology develops, it is expected that more affordable and more portable fingerprint recognition devices will become available, and finger-print recognition will be considered a safe and convenient personal identification system. Eventually, fingerprint recognition will be used to secure the safety and reliability of a variety of businesses in the industrial sector, including the personal devices and financial industry.

Fingerprint Recognition System is one of the most highly used methods for human Recognition which is automated biometric systems that have been only available in recent years. The quality of a fingerprint identification system not only depends on the accuracy of the system but also in the time that it takes to compute the answer.

REFERENCES

[14] Amit Chauhan, Aparna Gautam, Sourabh Kumar Singh an d Dr. S.K. Shukla, Gender inequity From the Quadrant of Lateral Finger prints among the Age Group Of 18-25
Years from the Population of The National Capital Region of India. International Journal of Civil Engineering and Technology, 8(4), 2017, pp.1402-1407

