ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Multi Server Authentication System using Minutiae Extraction and Clustering Algorithm

Aarati Mohare[1]
Computer Department
BSIOTR, Pune
Pune – India

Rohini Taware[2]
Computer Department
BSIOTR, Pune
Pune – India

Nupur Patil[3]
Computer Department
BSIOTR, Pune
Pune – India

Abstract: ***A biometric identity verification system tries to verify user identities by comparing some sort of behavioral or physiological trait of the user to a previously stored sample of the trait. The area of biometrics can therefore be denied as the task of automatically recognizing a person using his/her distinguishing traits like fingerprints, voice patterns, iris patterns, keystroke dynamics, etc. This project implements a verification system based on fingerprints. The input fingerprint pattern checks for a one matching in a database of fingerprint. The input image undergoes enhancement and thinning. The minutiae points (the points in a fingerprint image where the fingerprint ridges either end or split up into two new ridges) which forms the basis of the recognition algorithm is retrieved and the matching is done. A who accesses a network front different client terminal, can be supported by a credential server that authenticates the user by password, then assists in launching a secure environment for the user. Most of the People use the Email Services freely made available by various companies like Google, Yahoo, and AOL etc. It is very easy to hack these accounts and read the private mails. Moreover, it is not so convenient to log in every time to the specific mail server. The purpose of these concepts to secure to provide a facility to access accounts via multiple server through a single login and to provide security using the biometric fingerprint scanner.***

Keywords: Service server, Control server, AES, MINUTIAE Algorithm, Clustering Lingo Algorithm.

I. INTRODUCTION

The present invention provides a secure portable multi mail system for enabling an email user to manipulate emails of multiple servers. In one embodiment of the present invention, the secure portable email client system comprises a portable device capable of connecting to and being removed from an external host via an interface, and a secure portable email client program preinstalled on the portable device. The portable computer has an email client for viewing incoming email messages and composing outgoing email messages. The program the client is connected to a mail server and downloads all necessary letters on a local computer where further the mailing program allows to do with received mail anything you like - to read, delete, respond, catalogue, sort, and many other things.

This document sets out the high level vision for the "Email-Client". The Primary aim of this project is to provide a facility to access accounts via multiple server through a single login and to provide security using the biometric fingerprint scanner. The project aims at developing a system where the user can connect to a server using WLAN services. There can be two types of user, a mobile user and a desktop user. Every user has to register to the local server and create accounts for the specific mail server. On successful registration for a mobile user a key is generated which acts as a PIN code to the user which should be entered at the time of authentication. When the user logins to the server he/she has to register email ids for which he wants to view mails on his/her mobile. When a desktop user wants to login to the server he/she has to enter a user

© 2014, IJARCSMS All Rights Reserved

ID and password along with the fingerprint. Now whenever the user wants to view or compose mail he/she simply connects to the server. The user can now view all the received emails. The systems allow users to log in only once, providing Access to multiple applications without the user having to log into each email server separately. With a central Identity Management system, Password Synchronization can be implemented relatively simply, thus improving security and simplifying management. FMMS enables the user to access all of the email inbox, and he is authorized by requiring only one single authentication. With Password Synchronization, users' passwords are synchronized across all systems so that the user will only need to remember one password.

II. IDENTIFY, RESEARCH AND COLLECT DATA IDEA

There are many Mail Service Providers on the internet today like Yahoo, MSN, etc. Mails are one of the most popularly used services by all sectors of life, corporate as well as personal to contact each other. And that too with no restriction on location and of course free of cost.

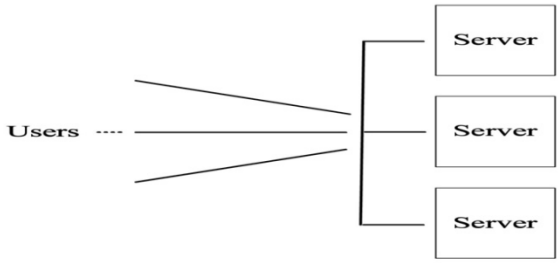


Fig 1: Current system at work as this interface client and sever

Different Mail Service Providers are popular in terms of different facility they provide say Inbox capacity, privacy, security, etc. So most of the people prefer their account on different service providers. The mainly disadvantages are the followings:

a. Waste of time creating new sessions of each service provider by logging into their respective domains.

b. More waste of Bandwidth and download capacity.

c. The client always needs to be online to check his mails or to do any other action related to it.

d. Have to remember all passwords.

III. PROPOSED SYSTEM

People have been exchanging emails for decades now, making email one of the most loved aspects of the Internet. And like anything else, sending email is most satisfying when the tools you use facilitate your work. You too will enjoy the power and simplicity of email client if you prefer the keyboard to the mouse, appreciates simplicity, but not at the expense of power, and are particular enough about your work environment to choose tools that provide maximum configurability. This is also the tool of choice for people that deal with large quantities of email and want a powerful, configurable tool. This aims at developing an Email Client application. The primary aim is to provide a scheduling facility to the Client.

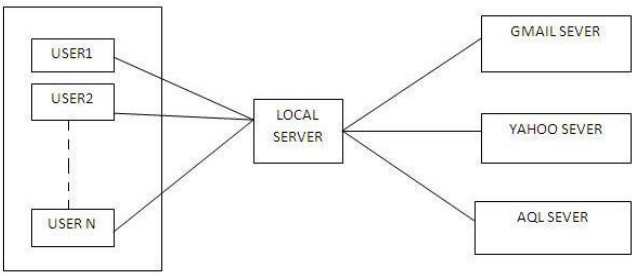


Fig2 : Smart Access Multi-Mail Server

© 2014, IJARCSMS All Rights Reserved

Current system facilitates the authentication for user, using the password based system. In current system users password data is shared with the single service provider system. The system helps to overcome the attacks of an offline dictionary by any hackers and server system is responsible for security of client's password data. Hackers will hack the offline dictionary when the server for authentication is compromised.In proposed system session key is established by the clients with the service server and function of control server is to support the service server for user authentication. The protection of the system is enhanced in architecture as a service server show to the user.

The local sever mainly characters as:

a. Maintains the database periodically after 15 minutes.

b. Caching the information.

c. Updating of Real Server database.

The Client characters as:

a. All clients store their information by registering themselves at the local server side.

b. Desktop user login using user id and password along with a fingerprint scanner.

c. Mobile user login using user id and password.

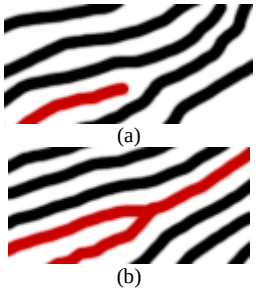
d. Perform mail operations.

IV. BIOMETRIC AUTHENTICATION

Fingerprints are the most used biometric technique for personal identification. There are two main applications involving fingerprints: fingerprint verification and fingerprint identification [1]. Usually associated with criminal identification, now has become more popular in civilian applications, such as financial security or access control. A More complex fingerprint features can be expressed as a combination of these two basic features. Minutiae matching essentially consist of finding the best alignment between the template (set of minutiae in the database) and a subset of minutiae in the input fingerprint, through a geometric transformation.

A. Minutiae extraction

Many fingerprint identification methods have appeared in literature over the years [1, 2, and 3]. While the purpose of fingerprint verification is to verify the identity of a person, the goal of fingerprint identification is to establish the identity of a person. In the past three decades, automatic fingerprint verification was being more widely than other techniques of biometrics such as face identification and signature identification. The most popular matching approach for fingerprint identification is usually based on lower-level features determined by singularities in finger ridge patterns called minutiae. In general, the two most prominent used features are ridge ending and ridge bifurcation (Figure3).

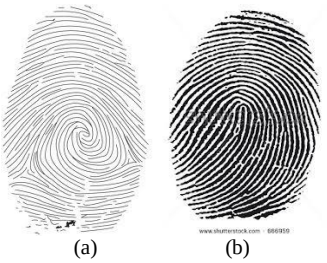


(a) (b)

Fig 3: Example of a) ridge ending and b) bifurcation.

© 2014, IJARCSMS All Rights Reserved

The two approaches of minutia extraction process can be found. The simplest and most used method is based on binarization and a ridge thinning stage. Due to a problem of the false minutiae introduced by thinning, some authors proposed direct grayscale minutiae extraction.



(a) (b)

Fig 4: Fingerprint image a) binarization and b) skeletonization [10]

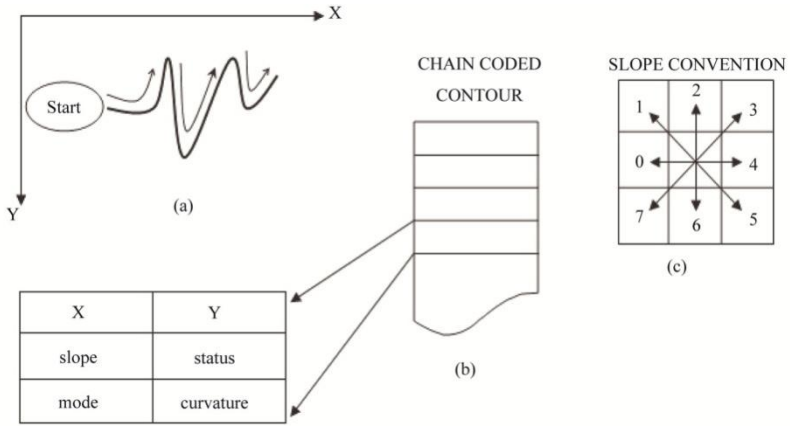


Fig 5:The minutiae points are determined by scanning the local neighborhood of each pixel in the ridge thinned image, using a 3×3 window.

The *CN* value is then computed, which is defined as half the sum of the differences between pairs of neighboring pixels pi and pi+1 [8]

$$CN_{(X,Y)}=\frac{1}{2}\sum_{i=1}^{8}|pi-pi+1|, p1=p9$$

Using the properties of the *CN* as shown in Table (Fig. 5), the ridge pixel can then be classified as a ridge ending bifurcation or non-minutiae point.

CN	Property
0	Isolated point
1	**Ridge is ending**
2	Continuing ridges
3	**Bifurcation**
4	Crossing

Table 1: Properties of the Crossing Number.

The main problem, in the minutiae extraction method using ridge thinning processes, comes from the fact that minutiae in the skeleton image do not always correspond with true minutiae in the fingerprint image. In fact, a lot of false minutiae are extracted because of undesired spikes, breaks, and holes. For this reason, time-consuming enhancement algorithms are required prior to thinning stage [9]. Minutiae extraction approaches, that work directly on the grayscale images, without binarization and thinning, were induced by these considerations [9, 10]:

a. Enhancement algorithms are time-consuming,

b. A significant amount of information may be lost during the binarization process,

c. Skeletonization may introduce a large number of false minutiae

d. Unsatisfactory results when applied to low quality images.

© 2014, IJARCSMS All Rights Reserved

B. AES Encryption

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data [4] to NIST during the AES selection process.[6] AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. Unlike its predecessor DES, AES does not use a Feistel network.

Rijndael is a family of ciphers with different key and block sizes.For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.[11] AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with a block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.The key size used for an AES cipher specifies the number of repetitions of transformation rounds that converts the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition is as follows:

a. 10 cycles of repetition for 128-bit keys.

b. 12 cycles of repetition for 192-bit keys.

c. 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds is applied to transform cipher text back into the original plaintext using the same encryption key.

C. Cluster Approach

Cluster analysis as such is not an automatic task, but an iterative process of knowledge discovery or interactive multi-objective optimization, when this is used in that we can access multi mail the types of the mails are divided in a cluster when it can be used in Lingo algorithmic concepts the user can easily find our mails like social mail, jobs mail etc. Cluster analysis itself is not one specific algorithm, but the general task to be solved. Popular notions of clusters include groups with small distances among the cluster members, dense areas of the data space, intervals or particular statistical distributions. Cluster analysis or clustering is the task of grouping a set of objects in such a way that objects in the same group (called a cluster) are more similar (in some sense or another) to each other than to those in other groups (clusters). It can be achieved by various algorithms that differ significantly in their notion of what constitutes a cluster and how to efficiently find them. It is a main task of exploratory data mining, and a common technique for statistical data analysis, used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics. The appropriate clustering algorithm and parameter settings (including values such as the distance function to use, a density threshold or the number of expected clusters) depend on the individual data set and intended use of the results.

V. CONCLUSION

This system provides more advantages than the previous system as well as this system provides high efficiency in term of computation and communication. Ordinary single-server, biometric based security application builds up by applied this system. It can be help in online services and it support federated enterprise setting, because a single central server handles the multiple service servers. In this paper, a minutia matching system has been described. The main problem in feature extraction section is quality of fingerprint images. Low quality areas of fingerprint occur large number of false minutiae points so in that system provides the easily can fetch the mail using multiple access sever at time user can handles multiple services.

© 2014, IJARCSMS All Rights Reserved

References

1. BEBIS G.DEACONU T. Fingerprint Identification Using Delaunay Triangulation, Proc. of Int. Conf. On Information Intelligence and Systems, pp. 452-459, Washington, DC, USA, 1999.
2. AMENGUAL J., JUAN A., PREZ J., PRAT F., SEZ S., VILAR J., Real-time minutiae extraction in fingerprint images,Proc. of the 6th Int. Conf. on Image Processing and its Applications, pp. 871–875, Ireland, 1997.
3. MEHTRE B. M., Fingerprint image analysis for automatic identification, Machine Vision and Applications 6, 2, pp. 124–139,India, 1993.
4. "Announcing The ADVANCED ENCRYPTION STANDARD (AES)". Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.
5. W. Ford and B S. Kaliski Jr.,(2000) "Server-Assisted Generation of a strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies.
6. John Schwartz (October 3, 2000). "U.S. Selects a New Encryption Technique". New York00 Times.
7. L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no.8, 1998, pp.777-789.
8. TAMURA H., A comparison of line thinning algorithms from digital geometric viewpoint. Proc. Of the 4th Int. Conf. On Pattern Recognition, pp. 715-719, 1978.
9. MALTONI D., MAIO D., JAIN A.K., PRABHAKAR S., Handbook of Fingerprint Recognition. Springer, New York, 2003.
10. MAIO D., MALTONI D., Direct Gray-Scale Minutiae Detection In Fingerprints, IEEE Trans. Pattern Anal. Machine. Intell, vol 19, pp. 27-40, USA, 1997. [5] Daemen, Joan; Rijmen, Vincent (9/04/2003). "AES Proposal: Rijndael". National Institute of Standards and Technology. p. 1. Retrieved 21 February 2013.
11. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay (May 2000). "The Twofish Team's Final Comments on AES Selection"
12. Achtert, E.; Bohme, C.; Kriegel, H. P.; Kroger, P.; Muller-Gorman, I.; Zimek, A. (2006). "Finding Hierarchies of Subspace Clusters". LNCS: Knowledge Discovery in Databases: PKDD 2006. Lecture Notes in Computer Science 4213: 446–453. doi:10.1007/11871637_42. ISBN 978-3-540-45374-

© 2014, IJARCSMS All Rights Reserved