Providing Security Using An Intelligent Mixing Fingerprints Technique With OTP Generation

R. Sri Gokulam\textsuperscript{1}, V. Loganayagi\textsuperscript{2}

\textsuperscript{1}Student, Dept. of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur.
\textsuperscript{2}Asst. Professor, Dept. of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur.
\textsuperscript{1}sriparice41@gmail.com
\textsuperscript{2}logu.vadivel@gmail.com

Abstract- Mixing Fingerprints technique is one of the biometric techniques, which is used to provide more security for the particular user to access their own application. In the registration process, the user has to provide two different fingerprints and these fingerprints are mixed to form a new mixed fingerprint image. This image acts as an (original) virtual identity for the user. Then during the login process, the user has to provide the same two fingerprints and it will be mixed again to produce the mixed fingerprint and compared with the original image. If the fingerprint is valid then the user is allowed to access the application. Otherwise the access gets denied. To mix the two different fingerprints, the fingerprints get decomposed into two components namely, (i) continuous component and (ii) spiral component. Then the Continuous component of one fingerprint gets combined with the spiral component of another finger and vice versa. To provide more security, OTP generation technique is proposed to generate two different One Time Passwords (OTP), one is sent to the User’s mobile number as SMS and another is sent as User’s Email ID. Only after authentication of mixed fingerprint, mobile OTP as SMS and E mail OTP, user is allowed to access their own application.

Keywords- Continuous component, Mixed fingerprint, OTP, Spiral component.

\section{I \hspace{0.5cm} INTRODUCTION}

Identification based on biometric techniques obviates the need to remember a password or carry a token. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.

The possibility of generating a template representing a joint identity by a mixing process has been explored. Specifically, it helps to create the digital identity by mixing the fingerprints of two individuals to generate a single fingerprint defining the joint identity. A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits irregularities in local regions of the fingertip, termed minutiae points. The distribution of these minutiae points, along with the associated ridge structure, is believed to be distinctive for each fingerprint.

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns.

\section{A \hspace{0.5cm} One Time Password (OTP) Generation}

OTP is a password that is valid for only one login session or transaction. OTP avoids the number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTP is that, in contrast to static password, they are not vulnerable to replay attacks.

\section{II \hspace{0.5cm} RELATED WORKS}

N. Ratha, J. Connell, and R. Bolle \textsuperscript{[10]}, “Enhancing security and privacy in biometrics-based authentication systems”}

Biometrics is a rapidly advancing field that is concerned with identifying a person based on his or her physiological or behavioral characteristics. The advantages of this technique are the hacker can’t attack the identities and it enhances the security level more than the password systems then it helps to identify the authenticated user to use the application.
The disadvantages are the biometrics does not change over time, but at the same time it has greatest liability and once a set of biometric data has been compromised, it is compromised forever. Hence it requires the repeatable noninvertible distortions to the biometric samples. R. Cappelli [2], “Sfinge: Synthetic fingerprint generator” The basic idea behind SFinge is simple: fingerprint shape, a directional map and a density map are generated separately then these three features are combined to obtain a fingerprint pattern, which is finally made more realistic by adding noise. In order to generate more impressions of the same finger, a master-fingerprint (i.e. a ridge pattern which represents the unique and immutable characteristics of a “synthetic finger”), is first generated then several synthetic fingerprints are randomly derived, starting from the same master fingerprint. A. Jain, A. Ross, and U. Uludag [6], “Biometric template security: Challenges and solutions” The biometric cryptosystem combines biometrics and cryptography at a level that allows biometric matching to effectively take place in the cryptographic domain, hence exploiting the associated higher security. Then convert fingerprint template (minutiae data) into point lists in 2D space, which implicitly hide a given secret (e.g., a 128-bit key). The list does not reveal the template data, since it is augmented with chaff points to increase security. The template data is identified only when matching minutiae data from an input fingerprint is available. N. Ratha, S. Chikkerur, J. Connell, and R. Bolle [11], “Generating cancelable fingerprint templates” Generate cancelable bit-strings (templates) from fingerprint minutiae to provide a simple mean to generate cancelable templates without requiring for pre-alignment of fingerprints. The main idea is to map the minutiae into a predefined 3 dimensional array which consist of small cells and find out which cells include minutiae. One of minutiae is taken as a reference minutia and other minutiae are translated and rotated in order to map the minutiae into the cells based on the position and orientation of the reference minutia. After mapping, set the cells in the 3D array to 1 if they include more than one minutia otherwise the cells are set to 0. A 1D bit-string is generated by sequentially visiting the cells in the 3D array.

III  BACKGROUND

When the virtual identity gets generated the two different OTP will be produced and used for secured authentication. This approach helps to avoid the hacking of passwords and also provides the better way to access the particular’s application in high level security.

III  BACKGROUND

When the virtual identity gets generated the two different OTP will be produced and used for secured authentication. This approach helps to avoid the hacking of passwords and also provides the better way to access the particular’s application in high level security.

Fig 1. System Model

The fingerprints can be decomposed into two components like continuous component and spiral component then the decomposed components can be pre-aligned for easy combination. The pre-aligned components of fingerprints can get recombined in the following manner: the continuous component of one fingerprint is combined with the spiral component of another fingerprint and vice versa. At the end of combining two different fingerprints, a new fingerprint image can be produced and this image can act as virtual identity for the particular user and stored in the database. If the fingerprint gets matched then the user is authenticated and allowed for next authentication process.

V  PROPOSED SYSTEM

In Proposed system, the process of generation of two different OTPs can be done for more secured authentication using Random key Generation algorithm. One OTP is sent to user’s mobile as SMS and another one OTP is sent to user’s mail-id.
A Modules

Registration

- Fingerprint Decomposition
- Fingerprint Pre-Alignment
- Mixing Fingerprints
- Generating and storing virtual identity

Login

- Fingerprint Decomposition
- Fingerprint Pre Alignment
- Mixing Fingerprints
- Generating and checking virtual identity

Authentication

OTP Generation

B Modules Description

Registration: In the registration phase, the two different fingerprints of single user can be scanned and combined to produce a new mixed fingerprint image which can act as a virtual identity of the user and gets stored in the database.

Login: The user should place the same two different fingers for scanning then the scanner detects the fingerprints of user and sends them to server to produce a new mixed fingerprint which is used to compare with the original identity of user.

Authentication: The mixed fingerprint obtained from login phase gets compared with the original identity gets stored during registration phase. If it gets matched then the user is authenticated and allowed for next step.

OTP Generation: - Authentication of mixed fingerprint gets valid then two different One Time Password (OTP) gets generated. One is sent to user’s mobile and another one is sent to user’s mail-id. After authentication of OTP the user is allowed to access the application in secured way.

Fingerprint Decomposition:-

The fingerprint can be decomposed into 2 components:

1. Continuous component
   It refers the ridges (curved lines) in the finger

2. Spiral Component
   It refers the splitted ridges (minutiae) in finger

Fingerprint Pre-alignment:

The decomposed components of fingerprints get aligned in correct sequence

Mixing Fingerprints:

The continuous component of one fingerprint gets combined with the spiral component of other fingerprint

Generating virtual identity

After combining the different fingerprints, new mixed fingerprint is obtained which can act as a virtual identity

VI IMPLEMENTATION

In the Banking application, the user needs to place two fingers for generating new virtual identity and it gets stored for further verification during login process. If the user gets authenticated then the two different OTP can be produced for secured authentication.
VII. CONCLUSION

In this work, the concept of “mixing fingerprints” can be utilized to generate a new identity by mixing two different fingerprints of single user. The mixed fingerprint representing a new identity can potentially be used for authentication because the mixed fingerprint is dissimilar from the original fingerprints, which can be stored in the database by the server for the verification during login process. Hence it is secured. The generation of Two Different One Time Passwords using Random Key Generation Algorithm helps to provide more secured authentication.

VIII. REFERENCES


