Design of Strong Password Algorithm based on Multiple Fingerprints

GENGYU GE and LILVE FAN

ABSTRACT

As fingerprint is unique, relatively stable and easy to collect, fingerprint recognition appears on mobile phone, combination lock and online payment in recent years. Usually fingerprint is used only once to verify a lock or other forms of authentication, so if someone else gets the correct fingerprint, the lock will be unlocked easily. It is because of the easy acquisition, like getting by fingerprint ink or silicon film, fingerprints are easily picked up by thieves or other criminals. This paper aims to solve this problem by designing some strong password algorithms based on multiple fingerprints and lists some practical applications.

KEYWORDS

Fingerprint Recognition; Multiple Fingerprints; Strong Password; Algorithm.

INTRODUCTION

Fingerprint identification technology is one of many biomedical identification techniques which refers to the use of human body’s inherent physical characteristics or behavioral characteristics for personal identification. As known to all, fingerprint, facial features, voiceprint characteristics and iris features can be used for biometric identification technology [1-3]. But the most widely used technology is fingerprint recognition. It is a commercial success that Apple Inc. launched a smart phone with fingerprint recognition that supports unlock and electronic payment via fingerprint recognition. With the development of IOT (Internet of Things) technology and its wide application in recent years, the smart home industry is extremely hot. Fingerprint identification lock is an important component of smart home, but its safety performance deserves our attention.

A fingerprint identification system includes several steps. First collecting a fingerprint and extracting eigenvalues in fingerprint images, then save the eigenvalues to the database or ROM storage, at last receiving ones fingerprint, repeat the first step and comparing with the pre-stored values in the database or ROM storage. The existing fingerprint verification method is collecting one fingerprint of ten fingers and verify only once. Unless wearing gloves all the time, people’s fingerprint can be extracted from anywhere like the surface of paper, keyboard and table. Also there are so many technologies that can easily crack fingerprint recognition, such as cloning fingerprints, high-resolution photos replacement of fingerprint.

Gengyu Ge, 948413217@qq.com, Lilve Fan, 942509669@qq.com, School of Information Engineering, Zunyi Normal College, Zunyi 563006, China.
The fingerprint identification system first takes the fingerprint image and then performs a series of preprocessing on the fingerprint image, extract fingerprint features that can be converted and compared with mathematical code. These features can be either ridge or valley form characteristics or detail or general characteristics. The computer converts these characteristics into the form of mathematical code stored in the sample database. When a fingerprint needs to be verified, the fingerprint characteristic code is compared with the sample code in the sample database, which is the feature matching [4, 5]. Finally, giving a matching result. Fingerprint identification system generally includes image acquisition, image preprocessing, feature point extraction and feature matching, as shown in Fig.1.

Fingerprint Image Acquisition

There are three categories of fingerprint image acquisition which are press fingerprint collection, fuzzy fingerprint collection and living fingerprint collection. Traditional fingerprint image acquisition method is mainly in the form of printing ink, most of the collected fingerprint images are indistinct. The quality of the image can vary widely depending on the power of the pressure, also leads to image defects. The fuzzy fingerprint collection is mainly aimed at the fingerprint left on the scene of criminal investigation and can be divided into three categories which are obvious fingerprints formed by sticking a finger on paint or blood, mound fingerprints formed by imprint on the material that can be formed, invisible fingerprints left on the object when the finger passes through sweat and other bodily secretions and touch on the object. Live fingerprinting refers to the direct use of instruments to collect images of people’s fingers. According to the principle of sensors, the acquisition equipment can be divided into several categories.

Optical acquisition equipment is commonly used in fingerprint collection, using the reflection principle of light and CCD that is a semiconductor device that converts optical images into digital signals. Solid-state sensor acquisition equipment is mainly divided into four categories, like silicon crystal sensor acquisition equipment, the pressure sensor acquisition equipment, electric field type acquisition equipment and temperature sensitive acquisition equipment. Ultrasonic scanning equipment uses ultrasound to scan fingerprints, receives different acoustic resistance values produced by ridge line and valley line to generate fingerprint image.
Image Preprocessing

The fingerprint image will be distorted because of the uneven light intensity, the stain, the molting aging or the skin scar. The purpose of image preprocessing is to reduce the influence of various factors on the image. Image preprocessing directly affects the correctness of subsequent feature extraction and matching. The general pretreatment techniques mainly include image enhancement, binarization, refinement, etc.

Image enhancement generally includes normalization, direction drawing estimation, image segmentation and filtering enhancement. Binary is to convert a grayscale fingerprint image into a binary image with only black and white gray values. The refinement is to frame the image based on the binarization image, and the black ridge segment is divided into a single pixel width.

Fingerprint Feature Extraction

A fingerprint refers to a line that occurs on the front of the head of a person’s fingers. The grain lines are arranged regularly to form different patterns, the starting point, end point, junction point and branch point of the striation line are detail characteristics of the fingerprint. Feature extraction is a form of digital code which can fully represent the uniqueness of the fingerprint image by means of the line direction, line breakpoints and bifurcation point. For the correctness of fingerprint feature matching, the extracted features are valid and the pseudo-characteristics are filtered out for various reasons. The two features of the fingerprint are used for fingerprint identification which is general characteristics and local characteristics.

General fingerprint characteristics can be recognized by naked eyes, mainly including patterns, singularities, and number of lines. The singular point includes the application and research of the core point and the triangle or delta point. The general characteristics are used to classify the fingerprint, but not the uniqueness of the fingerprint. As shown in Fig.2, the fingerprint image can be roughly divided into the following basic patterns, like arch, tented arch, left loop, right loop, double loop and whorl [6, 7].

Local characteristics refer to the details of the fingerprint image. Two pieces of the general characteristics of fingerprint image could be the same, but the local characteristics cannot be the same. It is the uniqueness of a fingerprint judgment standard, so local features are used to distinguish the fingerprint. The most common details are the following, as shown in the Fig.3, including ending, bifurcation, ridge divergence, dot, short ridge, enclosure.
Fingerprint Feature Matching

Fingerprint feature matching transforms extracted fingerprint image feature and compares with the samples in the fingerprint template database, then determines whether these two groups of characteristics are from the same finger. Feature matching requires robust features and matching algorithms need to be applicable to all kinds of fingerprint images. The current fingerprint matching algorithms are point pattern matching method, genetic algorithm matching method, Hough transform method and so on.

STRONG PASSWORD ALGORITHM

There are two algorithms to solve above problem that fingerprint may be acquired by others. One is special multimodal collecting fingerprints to unlock a combination of multiple code which made up of multiple fingerprints, another is multiple fingerprints matching in different sequences of time.

As shown in Fig.4, there are n (n>=2 and n<=10) fingerprint collection modules, each module corresponds to a preset fingerprint. Even if someone else has your fingerprints, he or she doesn’t know the arrangement sequence of the n fingerprints. Actually we can input n fingerprints as templates also less than n, as long as there are two or more fingerprint collecting modules to collect the same fingerprint. This method can greatly reduce the likelihood of password cracking.

In the same way, multiple fingerprints can be collected by one fingerprint acquisition module in different time and matching with the specified sequence of fingerprint characteristics in the templates database. The number of input errors can be set in the software, call the alarm if exceed a certain number of errors.
ACKNOWLEDGMENTS

This work was supported by education reform research project of Zunyi Normal College.

REFERENCES

6. Open_resultsAvg.asp