Comparison on the Security of Biometrics

Huichao Ye1, Roy Pei1, Zongyin Mo1, Qingmin Zheng1 and Huanzhong Chen1

1School of Information and Communication, Guilin University of Electronic Technology, Guilin 541000, P.R.China

Abstract. With the increasing requirements for public safety in modern society, the traditional authentication method is far from meeting the needs of protecting human safety. The biological features represented by human face, iris, veins, voiceprint, etc. play an increasingly important role in identity recognition, and are relatively found and get more attention. This article compares the advantages and disadvantages of the three biometric recognition technologies of human face, iris and vein, compares the security of each biometric recognition technology and makes a prospect of the biometric recognition technology.

1. Introduction

In the current era of big data Internet, a large amount of private information is stored online, and protecting information from being stolen has become a research focus. Biometrics technology is a pattern recognition technology[1] that a user owns and can express his own physiological or behavioral characteristics to identify himself. It has the advantages of safety, reliability and accuracy. The market share of common biometric recognition technologies is shown in Figure 1:

![Market share of biometrics technology](image)

Figure 1. Market share of biometrics technology

Global biometrics technology was first used in forensic fields such as forensic science. With the development of technology and the uniqueness of human biometrics that cannot be copied, biometrics is no longer limited to the field of security and is gradually being put into practice concerning airports, banks and various electronic appliances. Many foreign high-tech companies have tried to replace human credit cards or passwords with human biological features such as eye iris, fingerprints, palm prints, facial, and veins[2].

2. Types of Biometric Recognitions

2.1. Vein Recognition System

The vein recognition uses the hemoglobin in the blood to have infrared absorption characteristic[3]: When near infrared light is irradiated on the finger or palm, the absorption the hemoglobin in the subcutaneous vein of the finger or palm is higher relative to the skin, muscle and other physiological tissues. So it presents a black and white contrasting vein distribution image. After preprocessing such as normalization and denoising, filter enhancement and vein pattern segmentation, thinning repair,
then extracting its features, and then registering with the database in advance or the characteristic data
stored on the IC card is matched to determine the personal identity. Figure 2 shows the advantages and
disadvantages of vein recognition. Advantages of vein recognition:
a) High anti-counterfeiting: The characteristics of veins belong to the internal physiological
characteristics of the human body, they will not be worn, not exposed on the surface, and the
probability of being copied or stolen is very small. It has the advantages of high anti-
counterfeiting and high security.
b) Simplicity of identification: Compared with the high requirements for fingerprint humidity and
fingerprint integrity, vein recognition is not affected by whether the finger is wet, clean or
damaged, what the vein recognition scans is not the skin, but the underlying vein.
c) Public health: There is no need to touch the instrument with the finger during the vein recognition
process, and it will be more hygienic in public, which reduces the spread of infectious diseases to
a certain extent.

Disadvantages of vein recognition:
a) The hardware implementation cost is higher: compared with the fingerprint recognition module,
the cost of the vein recognition module is relatively high, especially the palm vein recognition
module.
b) Instability: So far, there is no really clear medical data and large-scale user data to determine
whether the vascular characteristics of the auxiliary witnesses remain the same for life. Therefore,
the dorsal vein of the hand may still change with age and physiology, which may cause
recognition errors.
c) Larger hardware: Compared with other biometric recognition technologies, vein recognition uses
infrared lamps to extract effective information. The presence of infrared lamps results in a larger
module and reduce portability.

Figure 2. Advantages and Disadvantages of iris recognition technology

2.2. Iris recognition technology

Human eye structure is composed of sclera, iris, pupil lens, retina and other parts. The iris is an
annular part between the black pupil and the white sclera. It contains many intertwined spots,
filaments, crowns, stripes, and crypts. And after the iris is formed in the fetal development stage, it
will remain the same throughout the life course. These features determine the uniqueness of the iris
characteristics, consequently determine the uniqueness of identification. The iris recognition
technology has the following four steps: iris image acquisition, image preprocessing, feature extraction,
and feature matching.

In 1993, Daugman proposed the theoretical framework of iris recognition technology[4], which
gives the iris image positioning method on how to normalize processing, feature extraction,
recognition and other parts and Laid the foundation for later research. Figure 3 shows the advantages
and disadvantages of iris recognition technology. Advantages of iris recognition:
a) Non-contact: Iris recognition uses specific cameras to obtain information. The human body does
not need to touch the equipment. Cleanliness reduces the probability of spreading infectious
diseases and enhances public safety.
b) High uniqueness: The iris is inside the eye and is unique. The iris characteristics of every two
people are not exactly the same, even the twins are not the same, and it is basically impossible to
be copied and modified
c) High stability: The iris hardly changes after the baby turns one year old.
Disadvantages of iris recognition technology:
a) Difficult to miniaturize: Iris recognition technology is difficult to miniaturize the image acquisition device in terms of hardware implementation.

b) Costly: Because it takes a lot of data to capture the iris, it is expensive to use a specific camera, which leads to high system cost.

c) Poor convenience: The iris recognition system is more difficult to recognize black eyes and has a strong dependence on light.

2.3. Face recognition technology

Face recognition technology is mainly carried out through the extraction and comparison of image features[5]. First, the system performs a similar search on the feature data of the extracted face image and the template stored in the database; then, by setting a threshold, the result exceeding the threshold is output; finally, the output features are compared with the template, and according to the similarities the confidence of the faces identity can be judged. Recognition technology is very complex based on these unique features, which requires artificial intelligence and machine knowledge learning systems.

Face recognition has been widely used in recent years, for example, face attendance, face social networking, face payment, etc. Machine learning is popular, making face recognition a higher level of application and accuracy. Figure 4 shows the advantages and disadvantages of face recognition. The advantages of face recognition technology:

a) Simplicity: No need for complicated operations, people can easily use and operate.

b) Non-contact: The user does not need to directly contact the device to obtain the image, which is clean and hygienic, avoiding the possible contact and infection of the disease.

c) Multiplicity: Multiple people can be identified at the same time.

Disadvantages of face recognition:

a) Easy to be deceived: Faces can be disguised through makeup, facelifts, etc., which makes face recognition techniques most likely to be deceived.

b) The rate of misjudgment is high: the position of the user's face and the surrounding lighting environment will affect the correct recognition.

c) Cost is expensive: The improvement of face recognition technology depends on the improvement of feature extraction and comparison technology. The more accurate the original data collection, the higher the cost of hardware equipment further improves then leading to high cost of system.

Figure 4. Advantages and disadvantages of face recognition

3. Summary and outlook

This article discusses the advantages and disadvantages of the three biometric recognition technologies, vein recognition, iris recognition and face recognition. From the above analysis, we know that the biometrics that can be used for identification have the characteristics of typical universality, uniqueness, robustness, and easy collection, that is, these biological characteristics are ubiquitous, and
different individuals are difficult to change and easy to collect, etc. Characteristics, and these characteristics have led to hidden security risks in protecting personal privacy. It is obvious that the safety of vein and iris recognition technologies are higher than face recognition technology. Table 1 shows the security of various biometric technologies[6].

Table 1. Biometrics technology performance comparison.

| Biometric | False Acceptance Rate | Easy to Use | Counterfeit Difficulty |
|-----------|------------------------|-------------|------------------------|
| Fingerprint | Fat Chance              | Comparatively Few | General |
| Palmprint  | Slim Chance             | 0.05        | General |
| Iris       | Fat Chance              | About10%    | Hardest |
| Face       | Slim Chance             | <0.2%       | General |
| Note       | Slim Chance             | 0.1         | General |
| Voiceprint | Slim Chance             | Slim Chance | Hard |

Different occasions have different requirements and methods for the protection of personal privacy of biometrics. For example, in public places with large traffic and small areas with high security requirements, technologies with lower rejection rates and lower false acceptance rates can be adopted. Technology, and the corresponding privacy protection methods.

With the increasing requirements for the accuracy and reliability of social security and identity authentication, a single biometric identification has been far from meeting the needs of society, which has hindered the wider application of this field. Since no single biometric recognition system is sufficiently accurate and reliable, the emergence of multimodal biometric recognition systems is an optional strategy.

References
[1] Prabhakar S, Pankanti S, Jain A K. Biometric recognition: security and privacy concerns[J]. IEEE security & privacy, 2003, 1(2):p.33-42
[2] Jain A K, Ross A, Prabhakar S. An introduction to biometric recognition [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 4-20
[3] Sun Xiaolin, Research on Finger Vein Image Pattern Extraction Algorithm [M], Jilin University, 2012
[4] Daugman J G. High confidence visual recognition of persons by a test of statistical independence [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993, 15(11): 1148-1161
[5] Zhang xin, xu yanjun. Automatic calibration of main facial feature positions in color images [J]. Chinese journal of image and graphics (2):138-143
[6] Zheng Fang, Escal Leuzi, Wang Renyu, Li Lantian. A review of biometrics recognition technology[J].Information Security Research,2016,2(01):12-26