International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21753

Classification and Performance of Biometric Authentication

Dr. Vijeet H. Meshram[*1], Dr. Ashish B. Sasankar[2]

[*1]Assistant Professor, Department of Computer Science, Dr. Ambedkar College, Nagpur, Maharashtra, India

[2] Principal, New Arts, Commerce and Science College, Wardha, Maharashtra, India

Article Info

Volume 7, Issue 5
Page Number : 16-20
Publication Issue :
September-October-2021
Article History
Accepted : 07 Sep 2021
Published : 14 Sep 2021

ABSTRACT

Out of the many authentication schemes in this paper we are trying to focus on the performance and classification of one of the techniques of authentication that is the biometric authentication. Although efforts of the entire international biometric community, the measurement of accuracy of a biometric system is far to be completely investigated and, eventually, standardized. The paper presents a critical analysis of the measurement of an accuracy and performance of a biometric system.

Keywords : Biometrics, Authentication, Performance.

I. INTRODUCTION

A. Classification

If the system has a large number of users, it might be a good idea to make some sort of classification of the sample before starting to compare it to the actual templates in the database. That way the number of necessary templates to be tested can be greatly reduced and therefore also the processing time.

Figure shows the classical fingerprint classification system that has been used by law enforcement agencies for decades. When a fingerprint was printed on card to be put into an archive, an expert first examined it to classify it. That way it was a lot easier to find a matching template when a new fingerprint arrived. Today the classification is done automatically and the method depends on the type of biometrics system used.

Figure 1. An example of biometric classification

B. Matching:

The matching procedure is the part of the verification process where the system tries to find a template in its database that is “sufficiently” alike the sample provided by the user. Due to the analog nature of the user sample, the system will probably not find a perfect match in its database, but rather a list of possible matches. If the system accepts the user or not, depends on some sort of security threshold set by the system administrator.

How the matching procedure actually is performed depend much on what type of biometrics system we are talking about. Generally, the system would try to find some key features in the user sample to match against the templates.

C. Transaction Completion and Storage

Depending on if the system is designed for verification or identification the result of the transaction can be to accept, to reject or to list possible matches. In the case of a verification system, it might be a good idea to keep a log of attempted verifications for security reasons and statistical reasons. Some systems might also update the template upon a successful transaction, this way the template quality will constantly improve and the system will be able to handle small natural changes to the biometric. For example scars in fingerprints, aging etc.

D. System Performance

System performance is a vague term and what it means depends much on what type of system it refers to. When talking about biometrics system performance, one usually means the probability that the system will accept authorized users and reject unauthorized users. As mentioned earlier a biometrics system usually has some security threshold setting that enables the system administrator to adjust the system to optimal performance.

The False Reject Rate (FRR) and the False Accept Rate (FAR) are often mentioned when describing biometrics systems. The FRR is, as one would guess from the name, the percentage of times the system refuses to accept an authorized user, and the FAR is the percentage of times that the system will accept an unauthorized user. The FAR and the FRR are closely connected. If the system administrator rises the security threshold, the false accepts will drop. Unfortunately, at the same time the FAR will increase since it also will be harder for the live samples of authorized users to match the higher demands. The reverse is also true, if the threshold is lowered the FRR will drop but the FAR will rise.

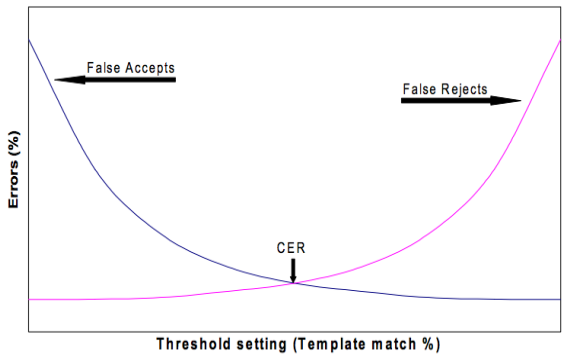

Figure 2. A typical performance curve

The Crossover Error Rate (CER), or as it is sometimes referred to, the Equal Error Rate (EER) is the point where the FRR and the FAR curves meet. Figure shows an example how these terms are linked together. When trying to set the security threshold to get optimal performance out of a biometrics system, it has been shown that the CER point is usually the best choice [1]. Of course this is not always the case, it depends on the type of security levels that are needed. If the system is intended to verify the identity of authorized personnel at Fort Knox, a few false rejects are probably to prefer compared to the risk of giving unauthorized personnel access to the facilities. On the other hand, if the biometrics system is used in an ATM the risk of a few false accepts are probably to prefer compared to the annoyance of the customers waiting in line if the system keep rejecting authorized users.

Another important term when talking about system performance, though often not mentioned by vendors, is Failure To Acquire biometric (FTA). The reason vendors donot mention this number is that it is usually a lot higher then the FAR and FRR. Say for example that the vendors of a fingerprint verification system claim their system has a CER of 0.0001%. That could be true in theory, but depending on the scanning device and the competence of user group, the FRR could actually be 20%. This is due to the fact

that the system might only be able to capture a good enough sample four times out of five.

II. ISSUES

There are also several other issues to consider when evaluating a biometrics system's performance, such as speed, user acceptance etc. You can, for example, not use a biometrics system in an ATM if it takes the system a couple of minutes to verify a user. And also, if the users do not trust the biometrics system to be accurate they will not be using the system to start with. Discussions over issues like these are usually collected together with the FAR, FRR, CER etc. into something called the Total System Performance (TSP).[2]

The fundamental barriers in biometrics can be divided into four main categories: (i) accuracy, (ii) scale, (iii) security, and (iv) privacy.

The critical promise of the ideal biometrics is that when a biometric identifier sample is presented to the biometric system, it will offer the correct decision. Unlike password or token-based system, a practical biometric system does not make perfect match decisions and can make two basic types of errors: i) false Match and ii) False non match.

1. False Match:

In the false match type of error the biometric system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database (in the case of identification/screening) or the pattern associated with an incorrectly claimed identity (in the case of verification).

2. False Non-match:

In the false non-matched type of error the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database (identification/screening) or the pattern associated with the correctly claimed identity (verification). It is more informative to report the system accuracy in terms of a Receiver Operating Characteristic (ROC) curve. Even ignoring the requirements of complete automation and assuming possibility of good biometric signal acquisition from a distance, it is easy to note that there is a need to bridge the gap between the current technology and performance requirements.

It is important to realize when compared to other pattern recognition systems, the false rejection of a user's claim by a biometric system is not a desirable outcome since a manual identification which is usually neither effective (e.g. to verify enrollment) nor feasible (e.g., large scale identification) has to be carried out. Practical biometric systems also have significant failures both in terms of failure to acquire (FTA) and failure to enroll (FTE).

III.REASONS FOR IMPERFECT ACCURACY

There are three primary reasons for the imperfect accuracy performance of a biometric system. They are i) Information Limitation ii) Representation Limitation and iii) Invariance Limitation. [3]

A. Information limitation:

The invariant and distinctive information content in the pattern samples may be inherently limited due to the intrinsic signal capacity (e.g.,individuality information limitationof the biometric identifier. For instance, the distinctive information extracted from the geometry is less than that of the fingerprints. Consequently, hand geometry measurements can differentiate fewer identities than the fingerprint signal even under ideal conditions. Information limitation may also be due to poorly controlled biometric presentation by the users or inconsistent signal acquisition. The measurements of a biometric identifier acquired through various means limit the invariance across different samples of the pattern. For example, information limitation occurs when there is

very little overlap between the enrolled and sample images in different poses and expressions. In such situation, even a perfect matcher fails to offer a correct matching decision. An extreme example of information limitation is when the person does not possess or cannot present exact biometric measurement needed by the identification system.

B. Representation limitation

An ideal representation scheme has to be designed to retain all invariance and discriminatory information in the sensed measurements. A typical practical feature extraction system based on simplistic models of biometric signal, fails to capture the richness of information in a realistic biometric signal, subsequently resulting in the inclusion of erroneous features and exclusion of true features. Consequently, a significant fraction of legitimate pattern space cannot be handled by the biometric system resulting in high FTA, FTE, FMR, and FNMR. For example, the individuality information contained in minutia-based representation of templates illustrates typical "poor quality" prints that cannot be processed by traditional minutiae-based identification systems, although the experts routinely use such smudged prints to make a reliable match decision. So, conventional representations and feature extraction methods are limiting the effective discrimination among the prints.

C. Invariance limitation

Finally, in a representation scheme, the design of an ideal matcher should perfectly model the invariance relationship in different patterns from the same class, even when imaged under varied presentation conditions. Again, in practice (e.g., due to non-availability of sufficient number of training samples, uncontrolled or unexpected variance in the collection conditions) a matcher may not correctly model the invariance relationship resulting in poor matcher accuracy.

IV. CONCLUSION

The user authentication, an essential part of a DRM system, determines whether the user is authorized to access the content. In a generic cryptographic system possession of the decrypting key is a sufficient evidence to establish user authenticity. Cryptographic keys are long and random, (e.g., 128 bits for the advanced encryption standard (AES)) and they are difficult to memorize. So, the cryptographic keys are stored somewhere (for example, on a computer or a smart card) and released on the basis to any alternative authentication (e.g., password) mechanism, that is, upon assuring that they are released to the authorized users. Most passwords are so simple that they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks. Many of these limitations of the traditional passwords can be ameliorated by incorporating better methods of user authentication.

Biometric authentication is one such method which eliminates most of the limitations other systems have. In Biometric authentication individuals are verified on the basis of their physiological and behavioral characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. It is inherently more reliable than password-based authentication, because biometric characteristics cannot be lost or forgotten (ex: passwords being lost or forgotten); Biometric characteristics are extremely difficult to copy, share, and distribute (ex: passwords being announced in hacker websites) and require the person at the time and point of authentication (ex: conniving users denying having shared the password). Biometric gives no scope for forgery since it requires more time, money, experience, and access privileges and it is unlikely for a user to repudiate a person, the digital content using biometrics. Finally, the biometrics is no easier to break than another's; that is, all users have a relatively equal security level, hence "easy to guess" biometrics, that can be used to mount

an attack against them, are relatively absent. Thus, biometrics-based authentication is a potential contender to replace password-based authentication, either by establishing the complete authentication mechanism or by securing the traditional cryptographic keys that contain the multimedia file in a DRM system.

Multiple biometric characteristics have been in use in various applications. Each biometric has its strengths and weaknesses, and the choice of the biometric depends on the application. A single biometric can not be expected to effectively meet all the requirements (e.g., accuracy, practicality, cost) of all the applications (e.g., DRM, access control, welfare distribution). In other words, no biometric is "optimal." The match between a specific biometric and an application is determined on the basis of the requirements of the application and the properties of the biometric characteristics.

Table 1. Comparison of Various Biometric Technologies Based on the Perception of the Authors. High, Medium, and Low are Denoted by H, M, and L, Respectively [4]

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Finger Print	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

V. REFERENCES

[1]. Whalberg M., "Biometric Security – Integration of Biometric Devices inSolaris", University of Umea, 2000

[2]. Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, and Arun Ross Michigan "Biometrics: A Grand Challenge", State University, IBM T. J. Watson Research Center,

[3]. Nazeer Unnisa Nazima, Shahana Tanveer ,Abdul Majeed, "Secure Public Key Protocol for Ad-Hoc Wireless Networks", International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 6, Decembers 2012 www.ijcsn.org ISSN 2277-5420.

[4]. Soutar, Biometric System Security White Paper, Bioscrypt [Online]. Available: http://www.bioscrypt.com

Cite this article as :

Dr. Vijeet Meshram, Dr. A.B. Sasankar, "Classification and Performance of Biometric Authentication", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 5, pp. 16-20, September-October 2021. Available at doi : https://doi.org/10.32628/CSEIT21753
Journal URL : https://ijsrcseit.com/CSEIT21753