Study on Face Recognition Technology Applied in Library Access Control System

-- Taking the Library of UESTC as an Example

Hengyi Guo [a], Xueyan Cao [b]

University of Electronic Science and Technology of China, Chengdu 611731, China.

[a]guohy@uestc.edu.cn, [b]caoxy@uestc.edu.cn

Keywords: Access control system; face recognition; library; statistical analysis.

Abstract: As an important branch of artificial intelligence, face recognition (FR) technology has the characteristics of anti-counterfeiting and non-repudiation. Applying this technology to libraries can meet the needs of libraries to fast and accurately identify readers. In this work, we investigate the FR system deployed in the library of the University Electronic Science and Technology of China (UESTC), from the perspective of data mining. After properly modeling the operating data, we propose certain parameters for evaluating the operating status of the FR system, and illustrate how to adjust the related threshold to maintain a stable operation of the FR system. The analysis method presented in this work can be used as a reference by other libraries when deploying FR systems.

1. Introduction

Face recognition (FR) technology is an important branch of artificial intelligence (AI) [1-4]. It recognizes individuals according to their biological features obtained by non-contact image capture. FR technology is widely used in practical applications due to its high recognition speed and accuracy. On the other hand, various reader-oriented services provided by university libraries, such as access licensing, lending, training room reservations and borrowing, etc., require fast and accurately identify readers. Therefore, it is natural to apply FR technology to university libraries.

In our previous work [5], we did a detailed analysis on the needs of the FR technology with the library as the user side. In addition, for the FR technology, we investigated its technical maturity, manufacturing maturity and maturity of the mainstream products in the market. We concluded that FR technology has a great potential to be used in libraries. However, due to the lack of operating data of the FR system, our analysis of the FR technology in [5] was mainly carried out from a macro perspective. On the contrary, from the perspective of data mining, this work is carried out by analyzing the operating data of the FR system deployed in the library of the University Electronic Science and Technology of China (UESTC). We propose certain parameters for evaluating the operating status of the FR system, and illustrate how to adjust the related threshold to maintain a stable operation of the FR system. The analysis method presented in this work can be used as a reference by other libraries when deploying FR systems.

2. Application of Face Recognition Technology in Library

2.1 A Brief Introduction to the Face Recognition System

The FR system usually includes four parts: face detection, face capture, FR, and face feature analysis and comparison. The core of the FR system includes face image acquisition, face feature extraction, and face image recognition [6]. Face detection is the basis of FR. It means that when the FR device captures an object in an image, it can detect and analyze the image to determine whether it is a human face. Simple face detection technology is currently more used in shooting equipment,

which is convenient for users to focus and beautify before shooting. In addition to face detection, FR needs to further analyze the detected face and compare it to the database and finally gives the comparison result. These functions of FR technology can lead to more applications, such as the authentication of legitimate users.

2.2 Advantages of Face Recognition Technology in Library Applications

At present, there are two main ways to apply FR as an authentication method [7]: One is to verify "A is A", called the 1:1 authentication mode, which is used for static comparison between features and ID photos; the other is to verify "someone is A", called the 1:N matching mode, which is used to find and match the verified person in multiple known legitimate users. The first mode works faster and is more accurate, and it is widely used in airports and train stations. On the other hand, the second mode is more convenient for users and more suitable for the scenario that the number of users is relatively stable and the user information is relatively fixed. Thus, the second mode is very suitable for university libraries. Using FR in the library access control system can not only ensure the security of the library, but also bring a more convenient and efficient entry experience to the readers [8].

To the best of our knowledge, up to now there is only a small number of libraries that use FR as a way for readers to get in and out [9]. There are three main reasons for this situation: First, the traditional way of using school card to get in and out of the library, has formed a basic habit in the reader community, and there are no big problems or contradictions; second, the FR technology is innovative and the equipment currently is costly; third, the existing literature mostly focuses on the qualitative analysis or simple quantitative analysis of the technical prospects [10, 11], lacking practical application cases and display of actual operating effect. That is why most libraries are still on the sidelines.

The way in which the library generally uses a card to verify the identity of the reader belongs to the type of item authentication. However, it is inconvenient and unreasonable to verify the legality of a reader's identity through an item: First, the reader who is authenticated must carry the authentication item with him at all times, otherwise, the reader's identity cannot be proved; second, the illegal reader may be easy to obtain legal rights whenever he gets the authentication item such as via borrowing. Instead, FR technology has the characteristics of "unplaceable" and non-invasive [12], which can better avoid the defects of the above-mentioned card authentication method. Using a reader's individual features, instead of other items, to do the authentication is very convenient for the reader. In addition, since these authentication features exist in the reader himself/herself, they cannot be borrowed or lost, and they are very unforgeable and non-repudiation. Therefore, using FR to carry out reader identification work will be more conducive to library services. The comparison between FR and card authentication is shown in Table 1. We believe the application of FR technology in libraries will become more and more extensive [5].

Table 1. Comparison between face recognition (FR) and card authentication

	User data collection difficulty	Recognition rate	Recognition speed	User information timeliness	User convenience	Anti-counterfeiting
FR	Easy	High	Fast	High	Very good	Very strong
Card	Very easy	High	Fast	Normal	Good	Weak

2.3 Application of Face Recognition Technology in Library Access Control System

After a full investigation of the FR technology, our library officially launched the FR system on March 1st, 2018. As a part of the library access control system, the FR devices allow readers to enter and exit the library through FR. According to the operating data from September 2018 to June 2019, readers successfully entering the library via FR and card authentication reach 1307883 and 684792 times, respectively. The readers much prefer using FR than using card, indicating a great success of

the application of FR technology in our library. The main workflow of the FR system used in our library is shown in Fig. 1. It consists of two parts: the offline process and the online process.

For the offline process part, the administrator first collects the photos of the legal readers, where part of these photos is imported from other departments in the university and the rest are obtained through on-site collection. Then, the FR system automatically processes the collected photo data, including face feature extraction, data integration, and so on. Finally, the processed data is stored in the database, and a one-to-one mapping between the face data and the identity of the reader is established in the database. In this way, the database created by the offline process can be used for data matching and identity authentication for FR in the online process.

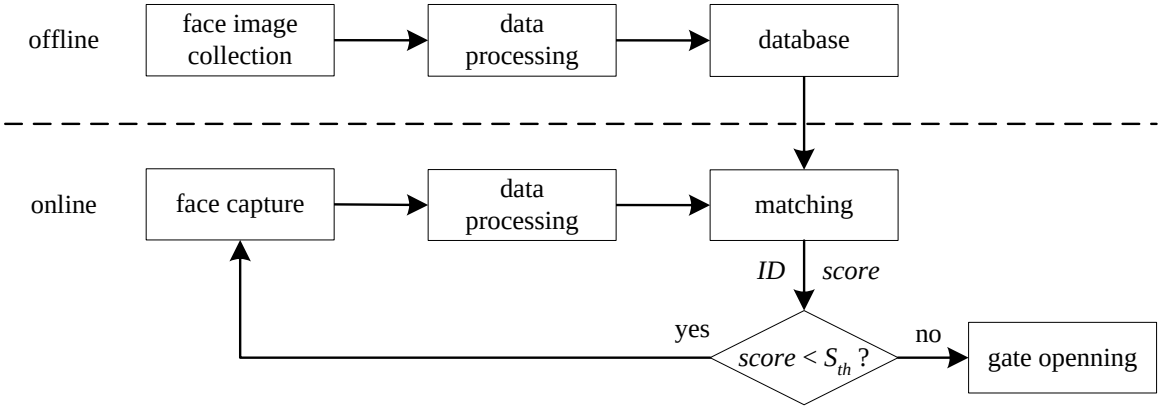

Fig. 1 The workflow of face recognition applied to library

For the online process part, after reaching the gate of the access control, the reader first performs FR, and the device captures the face of the reader. Next, the FR system processes the captured photo data, then matches the processed data in the database and returns the highest matching reader identity (*ID*) in the database along with the matching score (*score*). (Variables are denoted in italic form in this paper.) *ID* is a keyword that can uniquely identify the reader, such as student number, identity number, etc.; *score* is an integer belonging to [0, 100], and the larger the value, the higher the matching degree. Finally, the FR system compares *score* with the system's preset threshold S_{th}. If $score < S_{th}$ holds, the system considers that the reader's face photo is not sufficiently matched in the database, and the authentication is failed. In this case, the gate will not receive any opening signal, and the reader needs to try again after certain adjustment (e.g. adjust the capture angle). Otherwise, the system determines that the reader is successfully authenticated (the identity of the reader is *ID*), and sends an opening signal to the gate. The gate opens accordingly and will remain the openning state until the reader passes or the openning state lasts for 10 seconds.

3. Evaluating the Operating Status of Face Recognition System

3.1 Modeling Face Recognition Records

For the sake of simplicity, we model each FR record by a 3-tuple:

$$rec = (time, ID, score),$$

in which *time* represents the time when the FR authentication behavior occurs, and also the time when the record is generated; *ID* indicates the identity stored in the database which has the highest matching score with the reader under authentication; *score* is the matching score which belongs to [0, 100]. An example of 3-tuple FR records is shown in Table 2. The reader XX appears in both rec_1 and rec_8. Therefore, the FR record set of XX is $\{rec_1, rec_8\}$. Similarly, the FR record set of the readers YY and ZZ are $\{rec_2, rec_3, rec_4, rec_5\}$ and $\{rec_6, rec_7\}$, respectively.

Table 2. Example of 3-tuple face recognition (FR) records

FR record labelling	3-tuple record
rec_1	(2019-05-25 15:00:00, XX, 80)
rec_2	(2019-05-25 15:00:01, YY, 68)
rec_3	(2019-05-25 15:00:03, YY, 70)
rec_4	(2019-05-25 15:00:05, YY, 70)
rec_5	(2019-05-25 15:00:06, YY, 65)
rec_6	(2019-05-25 15:00:07, ZZ, 60)
rec_7	(2019-05-25 15:00:10, ZZ, 60)
rec_8	(2019-05-25 17:10:15, XX, 80)

Let n denote the number of the FR records of interest. The set of these records is denoted by $R = \{rec_1, rec_2, \ldots, rec_n\}$, with $rec_i = (time_i, ID_i, score_i)$ being the i-th record in R. For any record rec_i in R, define three functions: $time(rec_i) = time_i$, $ID(rec_i) = ID_i$, and $score(rec_i) = score_i$. Recall that S_{th} is the preset matching score threshold. If $score(rec_i) < S_{th}$ holds, rec_i is called a failed record; otherwise, rec_i is called a successful record.

3.2 Statistical Analysis of Face Recognition Records

For any FR record set R with n records, denote the number of successful records in R by $times\_suc(R)$. The successful authentication rate corresponding to R is defined by

$$rate\_suc(R) = times\_suc(R) / n.$$

For example, suppose R consists of the records in Table 2, and preset $S_{th} = 70$. Then, the successful records in R are $\{rec_1, rec_3, rec_4, rec_8\}$, and we have $times\_suc(R) = 4$ and $rate\_suc(R) = 0.5$.

As to the FR authentication, many factors will affect the matching degree of the captured face photos in the database, such as light, capture angle, and whether the reader under authentication changes the hairstyle and so on. Then, the reader may need to go through multiple failed attempts in a short period of time before finally succeeding and passing the gate. Besides, some readers may be curious about the FR system, and may thus perform multiple authentication attempts in a short period of time, regardless of whether the authentication is successful or whether the gate is open. Therefore, when computing the number of pass behaviors and pass rate of the readers via FR authentication, the multiple authentication actions (FR records) of the same reader in a short period of time should be regarded as belonging to the same passing behavior, as defined below.

Definition 1: Let T_{th} be the preset time threshold. Assume $A = \{a_1, a_2, ..., a_k\}$ is a non-empty subset of R satisfying $time(a_1) \le time(a_2) \le ... \le time(a_k)$. All records of A belong to the same pass behavior if and only if for any $1 \le i < k$, both $ID(a_i) = ID(a_{i+1})$ and $time(a_{i+1}) - time(a_i) \le T_{th}$ hold.

Definition 2: Assume A is a non-empty subset of R and all records of A belong to the same passing behavior. A is called a complete passing behavior set if after adding an arbitrary extra record from R to A, all records of A no longer belong to the same passing behavior.

To conveniently compute the number of pass behaviors and pass rate of the readers via FR authentication, we can partition the records of R into subsets $R_1, R_2, \ldots, R_m$, where each subset is a complete pass behavior set and m denotes the number of different complete pass behavior sets. Also, m is regarded as the number of pass behavoirs corresponding to R. The partition can be done with the following four steps.

Step 1: The records of R are sorted according to the lexicographic order of identities (ID). If the identities of any two records are the same, the one generated earlier (with smaller $time$) is ranked first. The result after sorting is denoted by $R = \{a_1, a_2, ..., a_n\}$.

Step *2:* Set $i = 2$, $m = 1$ and $R_1 = \{a_1\}$.

Step *3:* If a_i and a_{i-1} belong to the same pass behavior, add a_i to R_m; otherwise, let $m = m + 1$, and set $R_m = \{a_i\}$.

Step 4: Let $i = i + 1$. If $i > n$, terminate the process; otherwise, return to Step 3.

For example, preset $T_{th} = 5$ seconds, and assume that R consists of the records in Table 2. In the first step, all the records in R are sorted to get $R = \{rec_1, rec_8, rec_2, rec_3, rec_4, rec_5, rec_6, rec_7\}$. Then, the next three steps lead to $R_1 = \{rec_1\}$, $R_2 = \{rec_8\}$, $R_3 = \{rec_2, rec_3, rec_4, rec_5\}$ and $R_4 = \{rec_6, rec_7\}$. In this case, the eight records in Table 2 are partitioned into 4 complete pass behavior sets.

After partitioning R into subsets $R_1, R_2, \ldots, R_m$, for any subset R_i, $1 \le i \le m$, if it does not contain any successful record (i.e., $times\_suc(R_i) = 0$), the gate during this pass behavior never opens, and the reader fails to pass the gate. Otherwise, the reader at least successfully authenticates once, and the gate opens accordingly and remains the open state until the reader passes or reaches 10 seconds. In this case, it is reasonable to believe that the reader has successfully passed the gate. Based on these analyses, we define the number of successful pass behaviors by the number of R_i with $times\_suc\ (R_i) > 0$, denoted by $times\_pass(R)$. Moreover, the successful pass rate corresponding to R is defined by

$$rate\_pass(R) = times\_pass(R) / m.$$

To better understand the reader experience of using FR, we further compute the average number of authentications for one pass behavior, given by

$$ave\_per\_pass(R) = n / m.$$

Again, take the set of records in Table 2 as an example of R, and preset $S_{th} = 70$ and $T_{th} = 5$ seconds. In this case, $R_1 = \{rec_1\}$, $R_2 = \{rec_8\}$ and $R_3 = \{rec_2, rec_3, rec_4, rec_5\}$ correspond to the successful pass behaviors, while $R_4 = \{rec_6, rec_7\}$ corresponds to the failed pass behavior. Therefore, we have $times\_pass(R) = 3$, $rate\_pass(R) = 0.75$ and $ave\_per\_pass(R) = 2$.

Let R consist of the FR records from September 2018 to June 2019 of the library of UESTC. In addition, we preset $S_{th} = 62$ for the FR system. In our statistical analysis, we set $T_{th} = 5$ seconds. Then, we can get that the successful authentication rate is $rate\_suc(R) = 0.918$, the successful pass rate is $rate\_pass(R) = 0.989$, and the average number of authentications for one pass behavior is $ave\_per\_pass(R) = 1.131$. These results indicate that the FR system works well in the library of UESTC, coinciding with our observation on the actual operating status of the FR system. In general, we recommend to use these parameters, i.e., $rate\_suc(R)$, $rate\_pass(R)$ and $ave\_per\_pass(R)$, to evaluate the operating status of the FR system.

3.3 Adjusting the Matching Score Threshold

The matching score threshold S_{th} is the most important parameter which significantly affects the operating status of the FR system, while the time threshold T_{th} does not. In fact, according to our working experience, we generally set T_{th} as 5 seconds. After fixing T_{th}, for a given FR record set R, the calculation results of $rate\_suc(R)$ and $rate\_pass(R)$ are only affected by S_{th}, and $ave\_per\_pass(R)$ will remain a fixed value. Increasing S_{th} will reduce $rate\_suc(R)$ and $rate\_pass(R)$ accordingly. Therefore, S_{th} cannot be set too large, otherwise the working efficiency of the FR system will be reduced. However, if S_{th} is too small, it will inevitably lead to a high mis-recognition rate of the FR system. Here, "mis-recognition" means that for a successful FR authentication behavior, the identity of the reader determined by the system is not the current actual reader. A high mis-recognition rate of the FR system will severely impair its characteristic of anti-counterfeiting. Therefore, the S_{th} cannot be set too small.

Unfortunately, according to the FR records in R, the mis-recognition rate of the system cannot be computed because the case of mis-recognition cannot be detected by the system itself. When a mis-recognition case occurs, the system administrator can only know the situation after the mis-recognized reader reports the situation. However, not all mis-recognition cases are reported, resulting in an inability to accurately compute the mis-recognition rate of the FR system. Considering that the FR system with $rate\_suc(R) = 0.918$ and $rate\_pass(R) = 0.989$ in our library is

in good working condition--the reader can smoothly pass the gate via FR and the reported mis-recognition cases are also rare, 0.918 and 0.989 can be used as a good reference for the desired successful authentication rate *rate_suc** and successful pass rate *rate_pass**, respectively, when deploying the FR system in other libraries. In the following, we illustrate how to adjust S_{th} to achieve the preset *rate_suc** and *rate_pass**. The adjustment method can be used by other libraries.

At the beginning time, due to the lack of FR records, we can randomly set S_{th}. After operating the FR system for a period of time, we can collect enough FR records, denoted by *R*. According to the discussion in Section 3.2, we can compute *rate_suc*(*R*) and *rate_pass*(*R*) for each setting of S_{th}. Thus, an intuitive way is to enumerate S_{th} and then find the optimal S_{th} such that *rate_suc*(*R*) and *rate_pass*(*R*) respectively approach *rate_suc** and *rate_pass** as close as possible. However, we have a much faster way by using binary search [13]. Let *left* and *right* denote the minimum and maximum possible values of S_{th}, respectively (e.g., *left* = 0 and *right* = 100). In addition, assume S_{th} only takes integers from [*left, right*]. As an example, we now use binary search to find the maximum value of S_{th} such that *rate_suc*(*R*) < *rate_suc**. The binary search method contains the three steps below.

Step 1: Let S_{th} = (left + right) / 2 (S_{th} is rounded down to the closest integer). Then, calculate the corresponding *rate_suc*(*R*).

Step 2: If *rate_suc*(*R*) < *rate_suc**, let *left* = S_{th}; otherwise, let *right* = S_{th}.

Step 3: If *left* + 1 < *right*, return to Step 1; otherwise, return *left* and terminate the process.

The return value *left* of the above search process is the maximum value of S_{th} such that *rate_suc*(*R*) < *rate_suc**. Then, the optimal S_{th}, which makes *rate_suc*(*R*) approach *rate_suc** as close as possible, is given by either *left* or *left* + 1. This search process has a logarithm complexity, while the aforementioned intuitive way has a linear complexity, in terms of enumerating S_{th}. For example, for *left* = 0 and *right* = 100, this search process needs to enumerate S_{th} for at most 7 times, while the aforementioned intuitive way needs to enumerate S_{th} for 100 times.

4. Summary

In this work, we investigated the FR system deployed in the library of UESTC from the perspective of data mining. After properly modeling the operating data of the FR system to 3-tuples, we proposed three parameters, i.e., the successful authentication rate *rate_suc*(*R*), the successful pass rate *rate_pass*(*R*), and the average number of authentications for one pass behavior *ave_per_pass*(*R*), for evaluating the operating status of the FR system. Also, we illustrated how to adjust the matching score threshold S_{th} to maintain a stable operation of the FR system. The analysis method presented in this work can be used as a reference by other libraries when deploying FR systems. Moreover, this work together with our previous work [5] have a guiding role in the application and promotion of FR systems in libraries.

Acknowledgments

This research was supported by “Sichuan Information Management and Service Research Center Project in 2017, Information Service Model of University Library Based on Innovation and Entrepreneurship Training Project for College Students, No. SCXX2017ZD01”.

References

[1] Li Kai-fu, Wang Yong-gang. Artificial intelligence. Beijing: Cultural Development Press. 2017, p. 26-37.

[2] Huang Xiao-bin, Wu Gao. Development opportunity and change trend of library in artificial intelligence era. Library and Information. Vol. 06 (2017), p. 019-029.

[3] Baohebulide. The application, challenge, and developing trend of AI technology in library. Library and Information. Vol. 06 (2017), p. 048-054.

[4] Lu Ting-ting. From wisdom library to intelligence library: library development diversion in the artificial intelligence era. Library and Information. Vol. 03 (2017), p. 098-101.

[5] Qin Hong, Li Tai-feng, Guo Heng-yi, Xu Yi Case Study on Application of Face Recognition Technology in the Library. Journal of Academic Libraries. Vol. 06 (2018), p. 49-54.

[6] Yu Qing-li. A brief introduction to face recognition technology and its application in library management. Information and Communications. Vol. 11 (2017), p. 288-289.

[7] Dong Li, Zhao Wei-hua. Face recognition technology's application in university library management. Fujian Computer. Vol. 5 (2018), p. 37.

[8] Li Pei-rong, Xie Xie, Cui Xu, Li Shan-shan. Application and development of artificial intelligence in university smart library: based on face recognition technology and its algorithm. Library Science Research and Work. Vol. 7 (2018), p. 27-30.

[9] Wang Wei-qiu, Liu Chun-li. Library smart service function design and mode building in China based on face recognition technology. Library Science Research. Vol. 18 (2018), p. 44-50.

[10] Zhang Fan, Qin Yu-xuan. Technological landscape analysis of international face recognition. Science and Technology Management Research. Vol. 10 (2018), p. 28-35.

[11] Fu Yun-xia. Research on application of artificial intelligence in library construction. Library Science Research and Work. Vol. 9 (2018), p. 47-51,79.

[12] Zhang Jing-duan. Study on library access control system based on face recognition technology. Modern Electronics Technique. Vol. 18 (2016), p. 99-103.

[13] Information on: https://en.wikipedia.org/wiki/Binary_search_algorithm# CITEREFK nuth 1998.