Fast Fingerprint Rotation Recognition Technique Using Circular Strings in Lexicographical Order

Oluwole Ajala
Department of Informatics
King's Collage London
Email:oluwole.ajala@kcl.ac.uk

Moudhi Aljamea
Department of Informatics
King's Collage London
Email: mudhi.aljamea@kcl.ac.uk

Mai Alzamel
Department of Informatics
King's Collage London
Email:mai.alzamel@kcl.ac.uk

Costas S. Iliopoulos
Department of Informatics
King's Collage London
Email:c.iliopoulos@kcl.ac.uk

***Abstract*—Fingerprint authentication till date, remains the most reliable biometric technique. The bulk of research that has focused on fingerprint authentication, has however, neglected the rotational issues that arise with fingerprints resulting to incorrect orientation identification or effecting the process speed. This paper proposes a fast pattern matching technique that caters for orientation differences in fingerprints, by implementing a pre-matching stage called the orientation identification stage and then match the fingerprint image with a stored image. The fingerprint is intercepted with a series of scan circles and the minutiae information is derived. This information will then be translated into a string, having its starting point as the least lexicographical rotation value. This fingerprint string information is then matched against a database of stored images using approximate string matching techniques. The experiment was conducted on solving the rotation stage to prove the efficiency of this method, where the extracting and re-rotation is done in less than a second, with a linear time algorithm, yet practically sub linear in respect to the short extracted binary strings.**

***Keywords*—Biometrics; Fingerprint; Rotation; Pattern Matching; lexicographic;**

I. Introduction

Biometric is a word that is derived from the Greek words bios and metric, which means life and measurement consecutively. In other words, this translates into the study of measurable biological data. A biometric can be said to be a measure of physiological (eye, hair, fingerprint, hand recognition) and traits (voice and gait) features of an individual. Biometric identification comprises of a number of methods used to reliably verify the identity of persons based on either a single or a combination of biometrics. As no two individuals can possess exactly the same biometric characters, this authentication method is viewed globally as the most reliable [1] and [2].

Biometrics has to do with the metrics or statistical analysis of biological data which can be human traits or characteristics. Nevertheless, biometric identifiers are peculiar and unique to individuals; personal identification based on biometric data offer the most accurate means of identification, hence, among all other forms of biometrics such as eye, face, voice and speech, the fingerprint identification remains the most popular till date [2].

The complication of security increases when information is disseminated over a wide area network or larger number of devices and systems being shared by unrelated users. As more information on individuals and companies are placed in the cloud, user privacy protection becomes a fundamental requirement. Issues on integrity, confidentiality and user authorisation pose a major concern. Thus, the core principles of information security are compromised [3].

Fingerprints have provided an impeccable means of user authentication and personal identification for a long time [4], possibly dating back to the 19th century, when the records of fingerprint details of criminals in Argentina were released. It has long since been adopted not just for law enforcement purposes (forensics and police), but also for commercial purposes like financial transactions and most recently, it is used as an authentication method in mobile devices and computers.

Fingerprints are made up of minutiae, which are basically ridges and furrows in parallelism with each other. These minutiae form a complicated pattern that when impressed on a fingerprint scanner, leaves a print. These prints are matched to stored images on a database for either verification, authentication or both purposes [2].

The fundamental fingerprints that exist are whorl, loop and arch. However, a commonly used classification is the Henrys classification consisting of eight classes: Plain Arch, Tented Arch, Left Slant Loop, Right Slant Loop, Plain Whorl, Double Loop Whorl, Central Pocket Loop Whorl and Accidental Whorl [5]

A. Fingerprint Recognition and Pattern Matching

Each fingerprint is permanent and unique. This distinctiveness is derived by features such as ridges-ridge endings, ridge bifurcation, valleys and furrows referred to as minutiae which form a unique pattern. Recent studies have shown that the probability of two persons sharing same fingerprint is less than one in a billion, hence its uniqueness [2]. With regards to application, two kinds of fingerprint recognition systems exist. They are identification and verification. In the identification system, the query fingerprint is inputted and then matched against a computed list of stored fingerprints for resemblance [6].

In this case, the output will be understandably short or non-existent as no two fingerprints are alike. The verification system however, involves an input of query fingerprints with claimed identities, to be matched against already stored IDs (name and fingerprint) within a database to corroborate consistency. The system then outputs a result which can be either an affirmative or a negative message [6]. Fingerprint matching can be done with different methods:

- ***Correlation matching:*** This requires two fingerprint images, then a relationship between the corresponding pixels is determined [7].

- ***Minutiae matching:*** This is the most popular of all matching techniques. Here, the minutiae is stored as a set of points and subsequently matched with the original [8].

- ***Ridge matching:*** This matches the ridges in the finger. The ridges points on the finger are captured. This technique is mainly used when a problem arises with the minutiae matching technique resulting from poor quality fingerprint images [8].

B. Road Map

The organization of this paper is as follows. In Section I, we presented some background related to fingerprints. Section II presents a brief literature review. We present our approach in Section III. The experiment and the result analysis will be presented in section IV. Finally, we briefly conclude and state the future work in V.

II. Related works

Fingerprint recognition has been a core study since prehistoric times, leading to the proposal of several algorithms to developing an almost precise recognition system. Additionally, the memory and processor intensive computation issues has been discussed and addressed in some previous works [9].

Most of these recognition approaches hinge on the assumptions that the fingerprint impression was got from a vertically placed finger to produce a linear pattern. These previous works that have been grounded on the fingerprint minutiae recognition ignored to deliberate on the image distortions that can occur when obtaining a print.

For example, what happens if the finger was placed at an angle to the scanning device or even perpendicular to it, there would be an encumbrance in determining the fingerprint accurately, an issue that was noted with the minutiae matching technique.

However, some algorithms did cater for the rotation issue specifically, according to [10] which is a fingerprint matching and non-matching analysis for different tolerance rotation degrees in commercial matching algorithms. The most popular matching methods are the correlation-based method and the minutiae-based method. The study evaluated the three most popular biometric systems (Neurotechnology Verifinger 6.0 Extended, Innovatrics IDKit SDK and Griaule Fingerprint SDK 2007) and the effect of the fingerprint rotation degree on each system. The results showed that the false match rate (FMR) values will increase as the rotation degrees increases in each system where the Verifinger systems perform better than the other two.

In 2012, [11] defines the rotation invariant fingerprint identification system by applying preprocessing steps to minimize the misaligning between two fingerprint images such as rotation and scaling. Thus, the maximum correlation should be found after minutiae extraction. Also, they defined the false accept rate (FAR) and false reject rate (FRR) by threshold value, the downside of this technique is that it is based on the scanner [9].

In 2014 [12] proposed a fingerprint recognition method using image morphology and neural network through using preprocessing steps and wiener filter, then training the neural network with overall FRR of 8% and FAR of 8%. Nevertheless, they mentioned that a recognition error might accrue due to the variation in the finger placement on the reader during the fingerprint acquisition process.

To this effect, many algorithms have been written, implemented and modified. It is in rectifying the glitches of these orientation differences that the concept of lexicographical rotational algorithm was engineered as no previous work justifies the use of circular string matching and lexicographical rotational algorithm in fingerprint rotation and matching identification.

III. Our Approach

Our approach in comparison to the current state of art caters for orientation differences in fingerprints by using the lexicographical algorithm to determine a starting point in both the derived and stored print. This adds a significant improvement from the current state of art.

A. Stage 1: Orientation Identification

We start by extracting the binary circular string from the scanned image using the proposed extraction method in [13], over specified radii to produce binary strings in linear time; which in practical can be sub linear in respect to the short length of the extracted circular strings. Afterwards, a lexicographical order will be calculated for each extracted string to establish the starting point of the circular string in ascending order which is in linear time with respect to the length of the strings, which frames the scope of this paper.

B. Stage 2: Verification and Matching

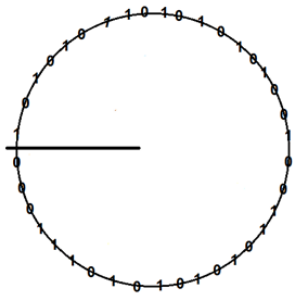
As with most other fingerprint recognition systems, a database with fingerprint information is kept. It is against this, that the queried fingerprint will be matched. Once stage 1 (the orientation identification stage) is complete, we can then simply re-orient the fingerprint impression to suit the stored format in the database, and extract more circular strings with lexicographical order to help this process. The matching algorithm then runs on an assumed dual image of the same orientation and magnitude. This is called the verification/confirmation stage and can be effectively carried out.

IV. The Experiment

The fingerprint image information in the database is represented in a binary format. The question of knowing the exact point to cut the circular string to determine the starting point for translating into linear binary strings then arises. This introduces the lexicographical rotation algorithm concept which is applied here. As a pre-processing step, the fingerprint image was enhanced through conversion to black and white,

resizing and thinning using Zhang-Suen algorithm [14].A part from the biometric special Databases and software was used as our dataset[15].

The experiment has been conducted on the first stage which is divided into two phases; first, extracting the circular strings in binary format; second, calculating the lexicographic order for the extracted strings to determine the starting point which we consider as the rotation of the fingerprint image (as shown in Figure 1).



Extracted String: 10101011010101001001101010101011100 0

Rotated String: 0101011010101001001101010101011100 01

Fig. 1: Extracting the Circuliar Strings using [13]

The experiment result shows in the table below (Table II) the extracting time over various radii and different string length is less than a second which is ultra fast. Furthermore, the processing time for the lexicographical order over the extracted circular strings is less than a second, regardless of the length of the string, therefore, the total for both phases is less than a second.

TABLE I. EXPERIMENT RESULTS 1

Extracted String Length	56	112	316	400	456
Extracting Time/Sec	0.0002	0.0001	0.0002	0.0003	0.0011
Starting Rotation Bit	5	0	5	2	4
Lexicographic Order Calculation Time/Sec	0.0012	0.0030	0.0065	0.0167	0.0500
Total Time of Extraction and Rotation/Sec	0.0014	0.0031	0.0067	0.0169	0.0511

Furthermore, the chart below shows that increasing the string length will slightly increase the time for calculating the lexicographical order. Therefore, the rotation time is not affected by the significant increase of string length which will help in increasing the accuracy.

A. Rotation and Speed

Since the scope of this paper is to concentrate on solving the rotation problem as shown in the table below, the speed of

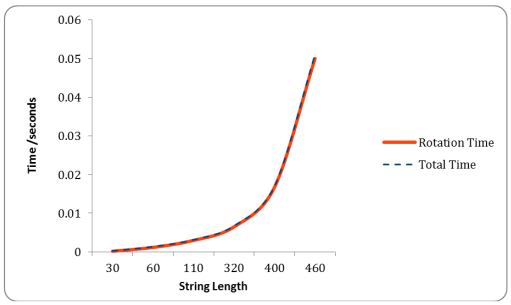


Fig. 2. Rotation/Total Time with Different String Length

the first stage which is orientation identification is not affected by the rotation degree of the scanned image. The table shows that processing the first stage with different angles for the same image is independent of the actual rotation degree and that is the strength of this approach.

TABLE II. EXPERIMENT RESULTS 1

Rotation Degree	Image	Radius	Cutting Point	Time
Original		70	7	0.014
90° (Left)		70	1	0.044
90° (Right)		70	4	0.043
180°		70	0	0.045

V. CONCLUSION AND FUTURE WORK

The quest for a better biometric based recognition system is nascent. Fingerprint being the most common of this based scheme therefore proves inevitable for periscopic investigation. This paper has addressed a notable challenge with fingerprint recognition and its subsequent pattern matching. It has proposed a potentially scalable algorithm-lexicographic algorithm, to tackle the issues of misleading orientations. With this resolved, any approximate circular string pattern matching algorithm can now run on the strings to produce an almost accurate result. Although our proposed matching algorithm runs in linear time and is accurate, faster pattern matching algorithms are needed to complete this cycle in recorded speed.

REFERENCES

[1] B. C. Liu, S. J. Xie, and D. S. Park, "Finger vein recognition using optimal partitioning uniform rotation invariant lbp descriptor," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[2] S. Sebastian, "Literature survey on automated person identification techniques," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 5, pp. 232–237, 2013.

[3] C. Bai, T. Zhao, W. Wang, and M. Wu, "An efficient indexing scheme based on k-plet representation for fingerprint database," in *Intelligent Computing Theories and Methodologies*. Springer, 2015, pp. 247–257.

[4] J. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern recognition*, vol. 47, no. 8, pp. 2673–2688, 2014.

[5] E. R. Henry, *Classification and uses of finger prints*. HM Stationery Office, 1905.

[6] N. A. Mngenge, L. Mthembu, F. V. Nelwamondo, and C. H. Ngejane, "An integrated approach to fingerprint indexing using spectral clustering based on minutiae points," in *Science and Information Conference (SAI), 2015*. IEEE, 2015, pp. 1222–1229.

[7] D. Peralta, M. Galar, I. Triguero, D. Paternain, S. García, E. Barrenechea, J. M. Benítez, H. Bustince, and F. Herrera, "A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation," *Information Sciences*, vol. 315, pp. 67–87, 2015.

[8] Y. Su, J. Feng, and J. Zhou, "Fingerprint indexing with pose constraint," *Pattern Recognition*, 2016.

[9] A. Agarwal, A. K. Sharma, and S. Khandelwal, "Study of rotation oriented fingerprint authentication," *International Journal of Emerging Engineering Research and Technology*, vol. 2, no. 7, pp. 211–214, 2014.

[10] A. Perez-Diaz and I. Arronte-Lopez, "Fingerprint matching and non-matching analysis for different tolerance rotation degrees in commercial matching algorithms," *Journal of applied research and technology*, vol. 8, no. 2, pp. 186–198, 2010.

[11] R. Mandi and S. Lokhande, "Rotation–invariant fingerprint identification system," *International Journal of Electronics Communication and Computer Technology (IJECCT)*, vol. 2, no. 4, 2012.

[12] R. Lakshmanan, S. Selvaperumal, and C. Mun, "Integrated finger print recognition using image morphology and neural network," *International Journal of Advanced Studies in Computer Science and Engineering (IJASCE)*, vol. 3, no. 1, pp. 40–48, 2014.

[13] T. S. I. C. o. P. P. PATTERNS 2015 and Applications, "A novel pattern matching approach for fingerprint-based authentication," pp. 45–49, 2015.

[14] W. Chen, L. Sui, Z. Xu, and Y. Lang, "Improved zhang-suen thinning algorithm in binary line drawing applications," in *Systems and Informatics (ICSAI), 2012 International Conference on*. IEEE, 2012, pp. 1947–1950.

[15] NIST, "Biometric special databases and software," http://www.nist.gov, 2015, [retrieved: 01.2016].

[16] OpenCV-code. (2015) Implementation of guo-hall thinning algorithm. [retrieved: 01.2016]. [Online]. Available: http://opencv-code.com/quick-tips/implementation-of-guo-hall-thinning-algorithm/

[17] J.-M. Guo, Y.-F. Liu, J.-Y. Chang, and J.-D. Lee, "Fingerprint classification based on decision tree from singular points and orientation field," *Expert Systems with Applications*, vol. 41, no. 2, pp. 752–764, 2014.

[18] Q. Zhang and H. Yan, "Fingerprint classification based on extraction and analysis of singularities and pseudo ridges," *Pattern Recognition*, vol. 37, no. 11, pp. 2233–2243, 2004.

[19] X. Chen, J. Tian, and X. Yang, "A new algorithm for distorted fingerprints matching based on normalized fuzzy similarity measure," *Image Processing, IEEE Transactions on*, vol. 15, no. 3, pp. 767–776, 2006.

[20] H. C. Lee, R. Ramotowski, and R. E. Gaensslen, Eds., *Advances in Fingerprint Technology, Second Edition*. CRC Press, 2002.