مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 123) 2024, pp. 29-45

Developing and valuation for Techniques Fingerprint Recognition System

Firas S. Abdulameer
Department of physics
College of Science, Mustansiriyah University, Baghdad, Iraq
firasalaraji@uomustansiriyah.edu.iq

Abstract:

The distinctive patterns observed on human fingertips are a result of the combination of ridges and troughs present on the skin surface. These patterns achieve their complete development during the period of pregnancy and remain stable throughout an individual's lifespan. Fingerprints refer to the impressions formed by the unique patterns present on the fingertips. Bruising resulting from accidental injuries, such as cuts and burns, can temporarily compromise the visibility of fingerprints. However, after the lesion has fully healed, the original patterns will be restored. Fingerprint recognition is a highly dynamic and extensively researched domain within the realm of biometrics. The word refers to the abbreviated form of the computational technique employed to ascertain the concordance between two distinct human fingerprints. In this naturally tough pattern recognition issue, it is imperative to minimize two error rates: the False Accept Rate (FAR) and the False Reject Rate (FRR). These mistake rates are in competition with each other. The development of computing capabilities has facilitated the creation of Automated Fingerprint Authentication Systems (AFIS), leading to a substantial increase in research activity, particularly in the past twenty years. This article aims to provide a comprehensive review of the issue surrounding fingerprint recognition, including an analysis of its underlying design and implementation difficulties, along with an assessment of its potential future developments.

Keywords- Fingerprint Recognition, Biometrics, Security, Verification, Identification, Validation

1- Introduction

Fingerprints are a widely used kind of biometric identification and measurement, especially in law enforcement, where they have been used to solve crimes for over a century. Unfortunately, matching fingerprints presents a difficult challenge in terms of pattern recognition. Manual fingerprint matching is not only time demanding, but it also requires a significant amount of time for the education and training of experts [1]. Because of this, considerable progress has been made since the 1960s in the area of developing systems that are capable of doing automatic fingerprint recognition. Accessing the Internet or any other significant resource securely necessitates the use of authentication techniques that provide a high level of protection. However, research [10] suggests that users often select passwords that are easy to crack, reuse passwords across several websites, and regularly forget their passwords. According to a poll that was carried out by the NTA Monitor in the year 2002, frequent users of the internet have an average of 21 different passwords, 81% of users choose a password that is already being used, and 30% of users either write down their passwords or store them in a file. Automated identification verification through the use of fingerprint recognition [4, 3] is a useful option in these types of scenarios.

Throughout the course of history, there has existed a significant correlation between fingerprints and the field of criminology, namely within the realm of forensic science. The broad usage of automated fingerprint authentication systems in business and civilian contexts can be attributed to the combination of the inherent simplicity of fingerprint capture and the advancements made in developing more reliable and cost-effective systems. The Integrated Automated Fingerprint Identification System (IAFIS), which has been under the jurisdiction of the Federal Bureau of Investigation (FBI) in the United States since 1999, is recognized as one of the most extensive fingerprint recognition systems.

1-1 The use of fingerprints as a biometric

The empirical facts serve as the foundation for the concept of the uniqueness of fingerprints. On the other hand, Golfarelli et al. [6] constructed the optimal Bayesian determination strategy for a biometric verification system and discovered a theoretical equivalent error rate (EER) of 1.31 x10^{-5} for a hand-geometry-based verified system and of 2 x 10-3 for a face-based confirmation system. These numbers refer to the accuracy of the systems, respectively. These results were obtained for a biometric verification system that was based on hand geometry. Pankanti et al. [5] demonstrated the same thing, demonstrating that there is only a small chance that two fingerprints will correlate to one another.

1-2 Categorized and indexed of Fingerprints

Two subdomains are included in fingerprint authentication. The first is fingerprint verification, which asks, "Am I who I declare I am?" The second is fingerprint identification, which asks, "Who am I?" Fingerprint designation is the more challenging subdomain, requiring substantial indexing and fingerprint classification for fast retrieval.

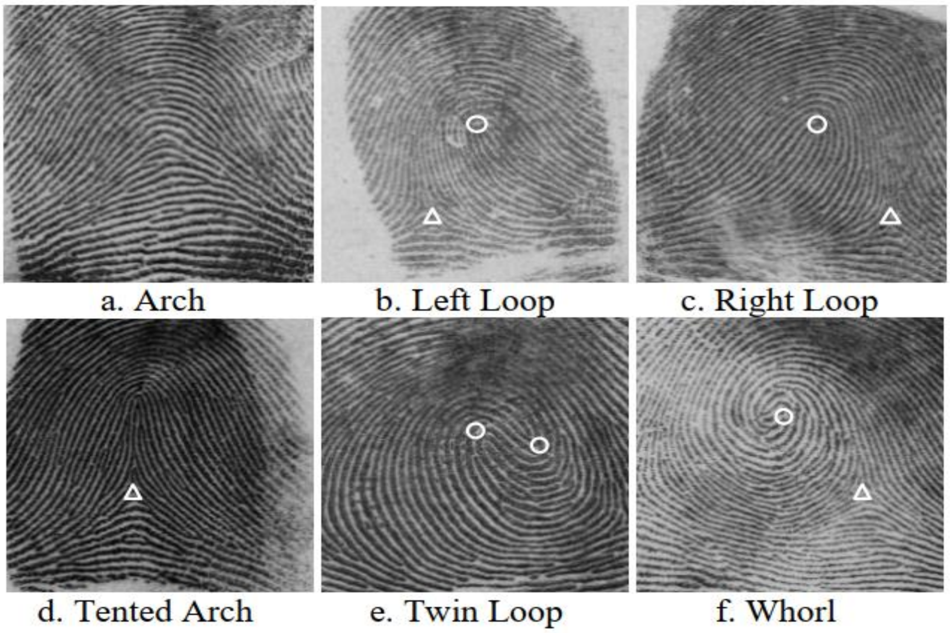


Fig. 1: Classification of fingerprints into six classes, with the core and delta of a fingerprint represented by circles and triangles.

The well-known "Henry System" is a fingerprint indexing approach that is designed to assist in the process of manually comparing fingerprints. This classification technique is the ancestor of virtually all other fingerprint classification methods that are now in use. For instance, the FBI uses a single form that can identify eight distinct types of patterns, such as accidental, radial loop, ulnar loop, double loop, central pocket loop, plain arch, tented arch, plain whorl, and radial whorl patterns. This form may also be used to determine whether or not a pattern is a radial whorl pattern [1]. Frequently, a whorl has a circular or spiral configuration. Arches have a form similar to that of a mound, whereas tented arches resemble a spire or spike in the center of the structure. Loops may have concentric hairpin or staple-shaped ridges, and their gradients may be designated as "radial" or "ulnar" based on the direction of the ridges. In contrast, radial loops slope toward the side of the hand where the thumb is located, whereas ulnar loops slope toward the side of the hand where the little finger is located. The classification and organization of fingerprints are a captivating area of study when it comes to detecting patterns, as there is limited diversity across different categories of fingerprint patterns, yet there is significant variation within each category. In this study Germain et al, outline a highly efficient approach for indexing extensive fingerprint databases, utilizing minute triplets. Furthermore, scholarly literature has proposed the implementation of improved classification systems, as exemplified by the work of Jain et al. [7].

2-Challenges of a Biometric Fingerprint Recognition System

The development and implementation of a Biometric Fingerprint Recognition System are not without their formidable challenges. One of the foremost concerns is the system's accuracy and reliability, as it must contend with variations in fingerprint quality, environmental conditions, and the natural aging of biometric traits. Ensuring that the system consistently delivers precise identifications and verifications is a constant challenge. Security and privacy also loom large, necessitating robust measures to protect stored fingerprint data from breaches and ensuring the system remains impervious to spoofing attacks. Scalability is another pressing issue, as the system must accommodate a growing number of users and fingerprint templates without compromising performance. Achieving user-friendliness while maintaining stringent security standards poses its own challenge, as does interoperability with existing infrastructure and applications. Environmental factors, like dirt or finger injuries, must be considered, and effective liveness detection techniques are required to thwart fraudulent attempts. Compliance with ever-evolving privacy regulations and standards, cost considerations, and the need for continuous updates and maintenance round out the multifaceted challenges faced by Biometric Fingerprint Recognition Systems. Addressing these challenges is paramount to harnessing the full potential of this technology while ensuring its security and effectiveness in a wide array of applications.

3-Components of the Fingerprint

The term "human fingerprint" pertains to the distinctive patterns of ridges present on the skin of a human fingertip, which can be utilized to characterize the imprint formed by these ridges. In this context, a recognition system is implemented that employs a hierarchical framework consisting of three tiers of attributes. In order to enhance comprehensibility, the subsequent enumeration presents the various tiers of features encompassed under this hierarchical structure: The pattern level is classified as Level 1, while the level of minute points is categorized as Level 2, and the level of pores and ridges is designated as Level 3. The great majority of AFISs include functionality derived from both Level 1 and Level 2 in their day-to-day operations. A level 1 characteristic would be something like the general form of the pattern that the unknown fingerprint has. This could take the shape of a whorl, a loop, or another pattern altogether. This shape can be utilized as a tool to help in the identification process of the fingerprint that has not yet been identified. Even though the amount of information that is offered is not adequate to permit individualization, it can be beneficial in reducing the number of options that are available when the search is being carried out. The specific friction ridge lines that have been plotted out are what are meant to be understood by the term "Level 2 features." This includes the overall flow of the friction ridges as well as important ridge route deviations (ridge characteristics known as minutiae), such as ridge ends, lakes, islands, bifurcations, scars, incipient ridges, and flexion creases. Also included in this is the flexion creases. In addition to this, this takes care of the general flow of the friction ridges. In addition, the term "Level 2 features" refers to both the general flow of the friction ridges as a whole as well as the specific ridges themselves in their distinct forms. The intrinsic detail that is present in a developed fingerprint, such as pores, ridge units, edge detail, scars, and so on, is referred to as "level 3 detail" [14]. This detail includes ridge units, edge detail, and scars. Ridge units, edge detail, and scars are all included in this particular detail. In order to extract Level 3 information from an image, you are going to need sensors that have a high resolution, preferably at least 1000 dots per inch. However, as shown in [8], when these features are combined with Level 1 and Level 2 capabilities, EER values can be lowered by a relatively small percentage (about 20 percent). Furthermore, as demonstrated in partial fingerprint recognition using Level 3 features is more likely to be successful [9].

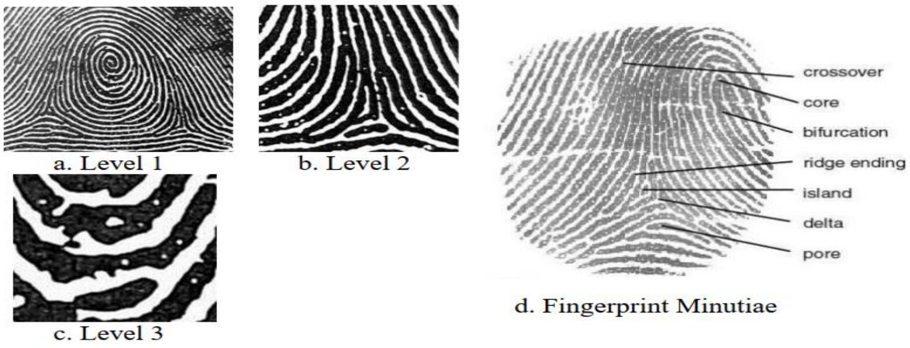


Fig. 2: Components of the Fingerprint

4-Sensing of Fingerprint

Fingerprint sensing comprises a diverse array of techniques, with offline scanning and live scanning being the two most prevalent approaches, both falling under the umbrella of live scanning. In the process of utilizing offline sensing, fingerprints are initially recorded on paper by the use of the "ink technique." Subsequently, these paper-based fingerprints are subjected to scanning via paper scanners, resulting in the creation of a digital image. The utilization of off-line sensing enables the retention of fingerprints for an extended duration compared to the utilization of on-line sensing. Offline sensing, also referred to as passive fingerprinting, is an alternative term for this methodology. The vast majority of AFISs use live-scanning, which is a technique for acquiring fingerprints directly through the use of an electronic fingerprint scanner. This method is responsible for the overwhelming majority of AFISs' applications. The great majority of sensors that are utilized in modern day applications fall into one of three broad categories: optical, solid-state, or ultrasonic sensors. Each of these three primary categories is a subset of the other two. In forensic and government applications, optical sensors that are based on frustrated total internal reflection (FTIR) are widely used to obtain live-scan fingerprints. FTIR is an abbreviation for frustrated total internal reflection. This is something that these kinds of sensors do on a daily basis. These particular fingerprint readers are the ones that get the most use overall out of all of the readers available. A key advancement in sensor technology was the invention of optical sensors that are based on fiber optics. This led to a reduction in the size of sensors as well as an increase in their portability. This innovation was documented in a patent application that was submitted in the United States [21], and it was granted.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 123) 2024, pp. 29-45

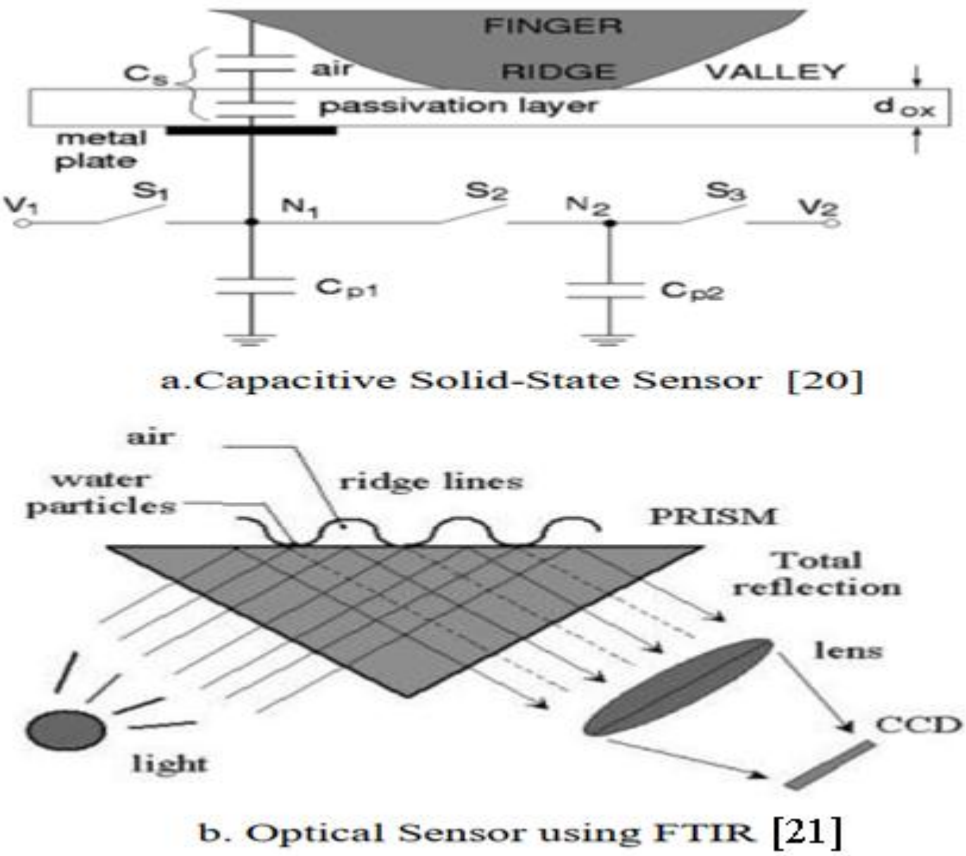


Fig. 3: Sensors of Fingerprint

The majority of commercial applications make use of solid-state touch and sweep sensors. These are the most frequent types of sensors. These devices, built on silicon, analyze the differences in the capacitance or disposal of the friction piles and ravines, as well as any other differences in their physical properties. Tartagni and Guerrieri , provide an explanation of a feedback capacitive sensing system that is capable of being implemented in standard 2-metal CMOS technology by making use of a sensor array that has a dimension of 200 × 200 elements. This can be done by deploying an array of capacitance sensors [22]. Jeong-Woo Lee et al.'s study discusses an additional form of solid-state sensor that is capable of creating fingerprints at a resolution of 600 dots per inch (dpi). Capacitive differences serve as the foundation for this sensor [20]. One example of the numerous commercially available bend instruments that are based on such low-power solid-state electronics is the Fujitsu MBF320. This sensor is just one example of the many.

The procedure of retrieving a latent fingerprint from a crime scene is an example of a one-of-a-kind application that makes use of off-line sensing [19]. Accidental impressions known as latent prints are created when friction ridge skin rubs against a surface. These impressions are brought about by the natural secretions of the eccrine glands that are present on skin and are utilized extensively in the field of forensic research. Despite the enormous advancements that have been complete in plain fingerprint identical, the subject of latent fingerprint similar remains to present a number of challenges. The process of matching latent fingerprints is more difficult than comparing regular fingerprints due to the low quality of the ridge impressions, the limited finger area, and the enormous amount of non-linear distortion that is present in the process.

5-Techniques for the Extraction of Features

It is necessary to have an appropriate representation of fingerprints in order to excerpt their structures for the goal of automating the process. The following characteristics ought to be possessed by this representation:

- Preserving the capacity of each fingerprint to differentiate between a number of different degrees of detail
- Capacity for simple computation
- Capable of being matched by computerized matching algorithms
- Unchangeable and unaffected by disturbances such as noise and distortions
- Representation that is both economical and condensed

Over the course of many years, a great number of different strategies for the extraction of features have been devised and effectively put into use. By utilizing image processing, one can extract fingerprint features using one of about four main types of techniques [11]. Without using the binarization and thinning processes, the first category of approaches directly pulls information from the gray-level picture [1, 23, 25, 34], while the second group of methods derives features from binary image profile patterns [15, 25, 26]. The omission of the word "process" distinguishes both types of approaches. Below, we'll go into more detail about both of these methods. The initial category of retrieval procedures extracts information directly from the grayscale image. The tertiary grouping of approaches [25, 28, 29] extracts minutiae by making use of machine learning, whereas the fourth and final category extracts minutiae by making use of binary skeletons. Both of these categories are divided into subcategories [2, 30].

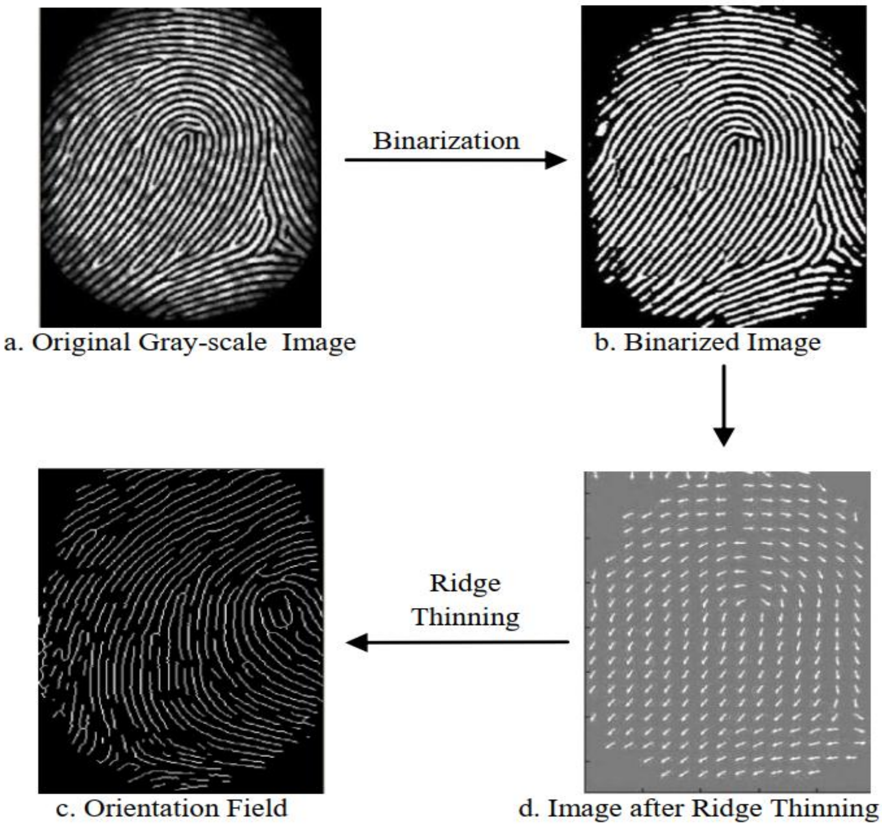
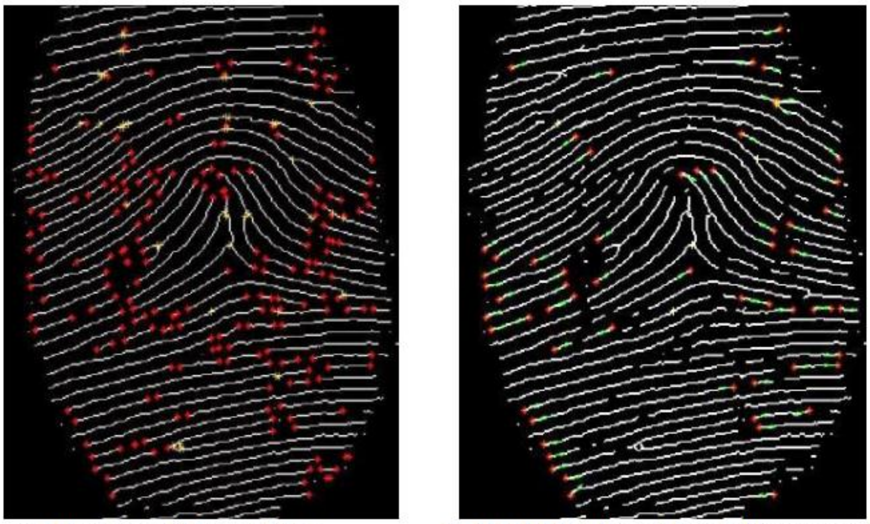


Fig. 4: Fingerprint Image of Minutiae Mining

Binarization is the process of taking an improved gray level image and transforming it into a binary image so that more feature identification may take place. This allows for more detailed feature identification to take place. Binarization techniques that are successful should be able to cut down on the quantity of information that is discarded while simultaneously simplifying the processing they require. Ratha et al, proposed a method for binarization that is based on the identification of a peak in gray-level cross-section profiles that are orthogonal to the orientation of the local ridges. This peak is used to determine whether or not the local ridges have a linear or nonlinear orientation [31]. An technique based on the Euclidean distance transform was

suggested by Liang et al. with the intention of achieving a near-linear temporal binarization of fingerprint images [27].
The practice of deleting unnecessary fingerprint ridge pixels until each ridge has only one pixel thick is referred to as fingerprint ridge thinning. This procedure can continue until each ridge has only one pixel thick. Ahmed and Ward conceived of the notion of a revolutionary iterative thinning technique [32], and You et al conceived of the idea of a multi-scale thinning strategy [33]. Both of these concepts were developed independently. Both of these suggestions have been made previously.



a.Minutiae after marking b. Real Minutiae after false removal

Fig. 5: Extraction of Minutiae
After the initial fingerprint feature extraction, some post processing is required in order to delete erroneous or spurious minutiae that were either introduced by earlier processing steps (such as thinning) or detected in highly damaged regions. These erroneous or spurious minutiae could have been caused by a number of different factors. Chen and Kuo proposed a method consisting of three steps that might be used to filter out inaccurate specifics [24]. This technique eliminated minutiae that had short ridges, minutiae that were located in noisy regions, and minutiae that were located in ridge breaks by making use of information regarding the orientation of the ridges. In their publication [30, 34, 35], Zhao and Tang introduced an extra method for removing all of the erroneous pixels that were created during the thinning

stage in order to make the process of minutiae filtering that came after it easier. This was done in order to improve the image quality.

6-Techniques for Reconstituting Fingerprints

Because the different impressions left by the same finger vary greatly (sometimes referred to as substantial intra-class variations), matching fingerprint pictures is a highly difficult challenge. In general, there are three main categories that fingerprint matching algorithms fall under:

A. On the basis of correlation When matching, two fingerprint images are placed on top of each other, and the correlation between corresponding pixels is computed for a variety of possible alignments (for example, multiple displacements and rotations). Both the Fourier transform, and the Fourier-Mellin Transform are methods that can be utilized to expedite the computation of correlation [12,13].

B. Matching Based on Features (or Matching Based on Details): The great majority of approaches to fingerprint identification use a matching system that is based on the characteristics of the fingerprint. When deriving minute details from the registered fingerprint picture and the input fingerprint image, the number of binarization points is one of the factors that is considered. Other examples of such details are ridge termination and ridge bifurcation. Ridge Thinning is a method that identifies a true fingerprint image by combining corresponding and minute elements from two different photos. In addition, Isenor and Zaky, present a method for matching fingerprints that is based on a network, whereas Jain et al. utilized a method for matching strings [17,2]. Fan et al present a method for verifying fingerprints that is based on the construction of a bipartite graph between model fingerprint feature clusters and query fingerprint feature clusters. This method is used to compare the query fingerprint feature clusters to the model fingerprint feature clusters [18]. Matching point patterns has traditionally been used to approach the problem of matching little features. Due of this, it has been the focus of a lot of research, resulting in the creation of a wide range of families of solutions, such as relaxation techniques, algebraic and operational research solutions, tree-pruning strategies, energy-minimization techniques, the Hough transform, and many others.

C. Image-based or Pattern-based Learning Options Matching pattern-based algorithms compare the fundamental fingerprint patterns of a candidate fingerprint with those of a previously stored template. These fundamental fingerprint patterns include local orientation and frequency, ridge shape, and texture information. Image-based algorithms perform a similar comparison but use a digitized image of the fingerprint instead of a scanned fingerprint. It is necessary that the photos be aligned in the same place, about a center point that is present on each image. After that, a graphical comparison of the candidate's fingerprint image and the template is carried out in order to establish the level of similarity.

Image correlation techniques can be either optical or computer-based, and both types are included in the image-based techniques. In recent times, numerous approaches that are based on transformations have also been investigated.

For example, Ito, et al provide a phase-based fingerprint image matching method that makes use of 2D discrete Fourier transformations[35], whereas Hamamoto explains a fingerprint matching method that is based on a Gabor filter. Both methods are used to compare and match fingerprint images [16]. The discrete Fourier transform is utilized in both of these different approaches.

7- System Design and Implementation Challenges

A fingerprint identification system is susceptible to making two distinct kinds of errors: a false match, which takes place when a match is discovered between images of two different fingers, and a false non-match, which takes place when photographs of the same finger do not result in a match. Both of these types of mistakes are considered to be errors. Therefore, one of the key aims that should drive the creation of a reliable fingerprint matching system should be to cut down on both of these different sorts of mistakes. This should be one of the primary goals that guides the development of a robust fingerprint matching system. It is impossible to decrease either one of the error rates simultaneously due to the fact that they are inversely reliant on one another. An additional feature of the design that is of the utmost importance is the safety of both the fingerprint recognition system as a whole and the database that stores fingerprint templates. When an individual's fingerprint template information is inappropriately utilized or shared after being received from one of these databases, this can pose a substantial risk to the individual's safety as well as their right to privacy. Even though there has been a considerable amount of research done on fingerprint recognition, there are still a huge number of research problems in this sector that have not been solved. Take, for instance:

- Completely robotic dormant fingerprint acknowledgement
- Detection of reformed or fake fingerprints
- Well-organized compression of fingerprint prototypes
- Mechanical generation of fake fingerprints
- Efficient automated fingerprint classification

The process of matching latent fingerprints introduces a whole new set of issues that are fundamentally different from those previously encountered. Latent fingerprints are often smudgy and fuzzy, catch only a tiny piece of the finger, and have severe nonlinear distortion as compared to full fingerprints taken using authorized methods such as live-scanning or inking during the registration process. This is because latent fingerprints are acquired by a different method. Additionally, only a small area of the finger is captured by latent fingerprints. During the enrollment process, these complete fingerprints will be collected. Because of this, they need to improve their extraction and matching procedures in order to make the process of latent fingerprint identification fully automated and eliminate the need for any kind of manual matching at all.

8-Conclusions

Since the beginning of the 20th century, researchers have extensively studied many aspects of fingerprint authentication. However, the widespread acceptance and implementation of technology for automated fingerprint identification has just recently emerged in mainstream society within the previous few decades. This can be attributed to the emergence of technology. The imperative to improve the security of automated fingerprint identification systems and mitigate error and failure rates has given rise to numerous captivating and innovative research prospects. The domains encompassed in this study comprise image processing, computer vision, statistical modeling, cryptography, and sensor creation. The need to enhance the security of automated fingerprint recognition systems and the growing demand to reduce their error and failure rates have directly led to the development of these prospects. These opportunities are a direct result of the growing demand for automated biometric recognition systems that reduce error and failure rates while simultaneously improving their security. These opportunities are a direct result of the rising demand for more accurate and reliable automatic biometric recognition systems. This demand is expected to continue growing in the foreseeable future. The results of our preliminary research reveal that fingerprints have been proved to be an excellent biometric, if not the greatest one; nonetheless, its full potential has not yet been explored by anybody. This is despite the fact that fingerprints have been shown to be an amazing biometric. Nevertheless, it is probable that challenges such as remote fingerprint authentication, real-time fingerprint identification in extensive applications encompassing billions of fingerprint records, the development of precise and secure fingerprint templates that can be revoked, and the scientific validation of fingerprint uniqueness will persist as significant obstacles in the foreseeable future.

References

[1] D. Palma and P. L. Montessoro, "Biometric-based human recognition systems: an overview," Recent Advances in Biometrics, pp. 1-21, 2022.

[2] U. Halici, L. Jain, and A. Erol, "Introduction to fingerprint recognition," in Intelligent biometric techniques in fingerprint and face recognition: Routledge, 2022, pp. 1-34.

[3] D. Maltoni, D. Maio, A. K. Jain & S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.

[4] P. Komarinski, Automated Fingerprint Identification Systems, Elsevier Academic Press, 2004

[5] S. Pankanti, S. Prabhakar, and A. K. Jain, ―On the Individuality of Fingerprints‖, IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010- 1025, 2002.

[6] Golfarelli M., Maio D., and Maltoni D., ―On the Error-Reject Tradeoff in Biometric Verification Systems‖ IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no.7, pp. 786-796,1997.

[7] A. K. Jain, S. Prabhakar and S. Pankanti, ―Matching and Classification: A Case Study in Fingerprint Domain‖, Proc. INSA-A (Indian National Science Academy), Vol. 67, A, No. 2, pp. 223-241, March 2001.

[8] Anil Jain, Yi Chen, and Meltem Demirkus, ―Pores and ridges: fingerprint matching using level 3 features,‖ 18th International Conference on Pattern Recognition, pp. 477 – 480, 2006.

[9] K. Kryszczuk, A. Drygajlo, and P. Morier, ―Extraction of level 2 and level 3 features for fragmentary fingerprints,‖ Proc. of the 2nd COST275 Workshop, Vigo, Spain, pp. 83-88, 2004.

[10] D. Florencio and C. Herley, ―A large-scale study of web password habits,‖ Proceedings of the 16th International conference on the World Wide Web, 2007.

[11] R. C. Gonzalez and R. E. Woods., Digital Image Processing, Prentice Hall, Upper Saddle River, NJ, 2002.
[12] Coetzee L. and Botha E.C., ―Fingerprint recognition in low quality images, Pattern Recognition, vol. 26, no. 10, pp. 1441-1460, 1993.
[13] Sujan V.A. and Mulqueen M.P., ―Fingerprint identification using space invariant transforms,Pattern Recognition Letters, vol. 23," no. 5, pp. 609-619, 2002.
[14] Q. Zhao, A. K. Jain, ―On the utility of extended fingerprint features: a study on pores, IEEE Computer Society Workshop on Biometrics, CVPR2010, San Francisco, U.S., June 18, 2010.
[15] R. S. Germain, A. Califano, and S. Colville, ―Fingerprint matching using transformation parameter clustering‖, IEEE Computational Science and Engineering, pages 42–49, Oct-Dec 1997.
[16] Y. Hamamoto, ―A Gabor filter-based method for identification‖, Intelligent Biometric Techniques In Fingerprint And Face Recognition, pages 137–151. CRC Press, Boca Raton, 1999.
[17] D. K. Isenor and S. G. Zaky, ―Fingerprint identification using graph matching, Pattern Recognition, 19(2):113–122, 1986.
[18] K.-C. Fan, C.-W. Liu, and Y.-K. Wang, ―A fuzzy bipartite weighted graph matching approach to fingerprint verification,‖ In Proc. of the IEEE International Conf. on Systems, Man and Cybernetics, pages 729–733, Oct 1998.
[19] Colins M.W., ―Realizing the Full Value of Latent Prints‖, California Identification Digest, 1992.
[20] J.-W. Lee, D.-J. Min, J. Kim, and W. Kim, ―A 600-dpi capacitive fingerprint sensor chip and image-synthesis technique,‖ IEEE Journal of Solid-State Circuits, Vol. 34, No. 4, April 1999
[21] Ichiro Fujieda, Yuzo Ono, Seijin Sugama, ―Fingerprint image input device having an image sensor with openings‖, United States Patent 5446290, August 29, 1995.
[22] M. Tartagni and R. Guerrieri, ―A fingerprint sensor based on feedback capacitive sensing scheme,‖ IEEE Journal of Solid-State Circuits, Vol. 33 Issue: 1, pages 133 - 142, Jan 1998
[23] L. Jinxiang, H. Zhongyang, and C. Kap Luk, ―Direct minutiae extraction from gray-level fingerprint image by relationship examination,‖ In International Conference on Image Processing (ICIP), volume 2, pages 427–430 vol.2, 2000.

[24] Z. Chen and C. H. Kuo. ―A topology-based matching algorithm for fingerprint authentication.‖ In IEEE International Carnahan Conference on Security Technology, pages 84–87, 1991.
[25] B. Bir and T. Xuejun. ―Fingerprint indexing based on novel features of minutiae triplets‖. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25(5):616–622, 2003.
[26] C. Wu, Z. Shi, and V. Govindaraju, ―Fingerprint image enhancement method using directional median filter,‖ In Biometric Technology for Human Identification, SPIE, vol. 5404, pages 66–75, 2004.
[27] A. B. Xuefeng Liang and T. Asano, ―A near-linear time algorithm for binarization of fingerprint images using distance transform, In Combinatorial Image Analysis, pages 197–208, 2004.
[28] S. Prabhakar, A. K. Jain & S. Pankanti, ―Learning fingerprint minutiae location and type, Pattern Recognition, 36(8):1847–1857, 2003.
[29] N. K. Ratha, S. Chen, and A. K. Jain, ―Adaptive flow orientation-based feature extraction in fingerprint images, Pattern Recognition, 28(11): 1657–1672, 1995.
[30] M. Ahmed and R. Ward, A rotation invariant rule-based thinning algorithm for character recognition, Pattern Analysis and Machine Intelligence, IEEE Transactions on, 24(12):1672–1678, 2002.
[31] X. You, B. Fang, V. Y. Y. Tang, and J. Huang Multiscale approach for thinning ridges of fingerprint. In Second Iberian Conf. on Pattern Recognition and Image Analysis, vol. LNCS 3523, pp 505–512, 2005.
[32] D. Maio and D. Maltoni, Neural network-based minutiae filtering in fingerprints, Fourteenth International Conf. Pattern Recognition, volume 2, pages 1654–1658, 1998.
[33] K. Ito, T. Aoki, H. Nakajima, K. Kobayashi and T. Higuchi, A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints‖, Proc. IEEE International Conference on Image Processing, 2005.
[34] P. Melzi, R. Tolosana, and R. Vera-Rodriguez, "Ecg biometric recognition: Review, system proposal, and benchmark evaluation," IEEE Access, 2023.
[35] A. M. Chowdhury and M. H. Imtiaz, "Contactless fingerprint recognition using deep learning—a systematic review," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 714-730, 2022.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 123) 2024, pp. 29-45

تقييم وتطوير تقنيات نظام التعرف على بصمات الأصابع

فراس صباح عبد الامير
الجامعة المستنصرية / كلية العلوم

مستخلص البحث:

الأنماط المميزة التي يلاحظها على أطراف الأصابع الإنسان هي نتيجة لمزيج من حواف وعمق الموجودة على سطح الجلد. تحقق هذه الأنماط تطورها الكامل خلال فترة الحمل وتبقى مستقرة طوال عمر الفرد. تشير بصمات الأصابع إلى الانطباعات التي تشكلها الأنماط الفريدة الموجودة على أطراف الأصابع. يمكن للكدمات الناتجة عن الإصابات العرضية، مثل الجروح والحروق، أن تؤثر بشكل مؤقت على رؤية بصمات الأصابع. ومع ذلك، بعد شفاء الآفة بالكامل، سيتم استعادة الأنماط الأصلية. يعد التعرف على بصمات الأصابع مجالًا ديناميكيًا للغاية ويتم بحثه على نطاق واسع في مجال القياسات الحيوية. تشير المقالة إلى الشكل المختصر للتقنية الحسابية المستخدمة للتأكد من التوافق بين بصمتين بشريتين متميزتين. في هذه المشكلة الصعبة المتعلقة بالتعرف على الأنماط، من الضروري تقليل معدلين للخطأ: معدل القبول الزائف (FAR) ومعدل الرفض الزائف (FRR). معدلات الخطأ هذه تتنافس مع بعضها البعض. لقد سهّل تطوير القدرات الحاسوبية إنشاء أنظمة التحقق من بصمات الأصابع (AFIS)، مما أدى إلى زيادة كبيرة في النشاط البحثي، خاصتا في العشرين عامًا الماضية. تهدف هذه المقالة إلى تقديم مراجعة شاملة للمشكلة المحيطة بالتعرف على بصمات الأصابع، بما في ذلك تحليل التصميم الأساسي وصعوبات التنفيذ، إلى جانب تقييم التطورات المستقبلية المحتملة.

الكلمات المفتاحية : تمييز بصمات الأصابع، البيومترية ، الأمن، التحقق، التعرف،التصديق.