Future Generation Computer Systems xxx (xxxx) xxx

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Fingerprint classification and identification algorithms for criminal investigation: A survey

Khin Nandar Win [a,b], Kenli Li [a,b,*], Jianguo Chen [a,b,*], Philippe Fournier Viger [c], Keqin Li [a,d]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[b] National Supercomputing Center in Changsha, Changsha 410082, China
[c] Harbin Institute of Technology, Shenzhen 518055, China
[d] Department of Computer Science, State University of New York, New Paltz, NY 12561, USA

ARTICLE INFO

Article history:
Received 30 June 2019
Received in revised form 18 September 2019
Accepted 27 October 2019
Available online xxxx

Keywords:
Classification
Clustering
Criminal investigation
Deep learning
Fingerprint
Machine learning

ABSTRACT

Fingerprint plays a fundamental role in community security and criminal investigation, such as forensic investigation, law enforcement, customs access and public security organs. This can also help to provide a more enjoyable and secure life to people. Various machine learning and neural network approaches have been proposed for fingerprint acquisition, detection, classification, and analysis. In this survey, we present an up-to-date literature evaluation of fingerprint classification algorithms and fingerprint application in the area of criminal investigation. Firstly, we discuss the characteristics of fingerprint and the application in criminal investigation. In addition, we analyze and compare machine learning algorithms of fingerprint in terms of classification, matching, feature extraction, fingerprint and finger-vein recognition, and spoof detection. Finally, we highlight the challenges in the fingerprint analysis and discuss the future directions.

© 2019 Elsevier B.V. All rights reserved.

1. Introduction

Fingerprint is the oldest biometric identification technologies for human beings and has been used since three thousand years for signing legal documents in China [1,2]. Generally, fingerprints can be categorized into three prints: patent (visible) prints, plastic prints and latent(invisible) prints for the investigation of the crimes [3]. Patent prints are formed if the fingers touched a surface and the finger ridges are left and merge with a colored material such as blood, grease, or ink, dirt, lubricant or some kind of oil and can easily be visible without using any extra microscope. Plastic prints can be observed when the finger rides are left on very sloppy things which can be used for the impression such as putty, paint, wax and soap, or it may be dust. Sometimes, it is also called impressed prints. It also can create three-dimensional impressed print. Because of this impression, it can be seen easily and can take the photograph for the print without doing any other development. It can also be used for detection of the spoof fingerprint. Latent fingerprint cannot be seen easily with the naked eye and can be made it detectable with dusting, fuming or some other chemical reagents. It can be created latent fingerprint by the sweat obtained from sebaceous glands of our bodies or water, salt and amino acids.

Fingerprint will always be the same throughout our lives until we died. In accordance with growing up, the size of our finger will be larger but the print on the finger will never change. Even if twins, the prints on both children will not be identical [4]. This is very valuable characteristic of the fingerprint. For this uniqueness, simplicity and its inexpensive, fingerprint is very popular and possible to use for the identification of the prints on not only a crime scene to remove or add a suspect from the consideration but also access authentication, customs access and public security organs for our social daily lives. At the scene of a crime, usually latent fingerprint is left accidentally [5,6]. Latent fingerprints can be collected from many different diversities of surfaces. And also, invisible fingerprints can be processed to produce visible prints for identification. These invisible prints usually created from skin oils. The prints can help the detectives to make a case against a suspect even the prints are partial, smudged or imperfect. Although many studies have been published on fingerprint classification and identification, according to our best knowledge there is no survey of these studies.

In this paper, we address this gap in the literature by presenting a survey of fingerprint classification and identification in the area of criminal investigation. Our paper is organized as follows. The nature of fingerprint and its essential and usefulness for criminal investigation are discussed in Section 2. Machine learning

* Corresponding author at: College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China.
E-mail addresses: knandarwin@hnu.edu.cn (K.N. Win), lkl@hnu.edu.cn (K. Li), jianguochen@hnu.edu.cn (J. Chen), philfv8@yahoo.com (P.F. Viger), lik@newpaltz.edu (K. Li).

https://doi.org/10.1016/j.future.2019.10.019
0167-739X/© 2019 Elsevier B.V. All rights reserved.

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

(a) Arch fingerprint (b) Loop fingerprint (c) Whorl fingerprint

Fig. 1. Three main fingerprint types (a) arch, (b) loop, and (c) whorl.

techniques and algorithms for the classification and identification of fingerprint are presented in Section 3. Conclusions and fingerprint research opportunities are given in Section 4.

2. Fingerprint in criminal investigation

In this section, we present the characteristics of the fingerprint and its usefulness in the investigation of crime scenes. As fingerprint is primarily used in the analysis of the crime and the identifying of the person, our paper is specifically focused on its usage of the inspection for the crime observation.

2.1. Fingerprint

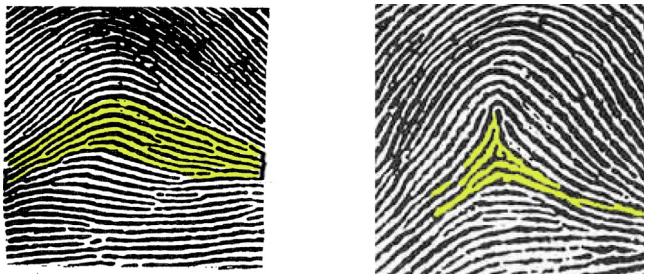
Fingerprint is the unique features of the skin. We can use it to identify a person because of its unique ridges and formation. The ridges of fingerprint are started to form during third to fourth month while we were fetus in pregnancy time [7,8]. The ridges are formed for the purpose of holding tightly and not to slip when we grip an object. They did regular patterns arrangement by themselves and uniquely have an arrangement and combination of ridge characteristics patterns. These patterns of friction ridges consist of many sweet pores rows. The sweat pores allow sweat and oil to get out from the gland. The fingerprints were formed if the sweat touched with other substance on the smooth surface.

2.1.1. Fingerprint types and patterns

Fingerprints can be left from the transfer of oils to the surface and also some substances such as paint, blood are left on the fingers or by putting an impression print in the soft substance [9,10]. We can find any identical fingerprints. Even though, the twins' fingerprints are different [11]. Generally, fingerprint patterns can be found in three categories: arches, loops, and whorls (see Fig. 1).

(1) Arch fingerprints.

Arches pattern can be found in 5% of all encountered fingerprints patterns. As its shape is the same as the name, the pattern is curved like the arch. In arches, the ridges move from one part to the another of the print pattern and there are no reversed turning ridges. Naturally, in an arch pattern, there will be no delta. But in some case, if the delta is formed, there will be no re-curving ridge between the core and the delta points [12]. Generally, we can find four categories of arch patterns: plain arches, radial arches, ulnar arches, and tented arches. The ridges of plain arches flow constantly from one surface to the another of the pattern [13]. The ridges start from one side of the impression and then slide to the other as a rise or wave shape into the print center. As for the radial arches, the ridges bend towards the thumb and there is one delta in the radial arches but any ridges are not re-curving. The ulnar arches is also the same with the radial arches except for bending the ridges towards the little finger. However, the tented arches have an angle, an push shape with the upward direction. They do not have the same flow pattern like the plain arches, and especially have distinct upward direction push pattern in the ridges near the middle of the print. Examples of Fingerprint Ridge Patterns and Characteristics patterns have been shown like in the following Fig. 6.



(a) Plain Arch (b) Tented Arch

Fig. 2. Arch fingerprint patterns.

(2) Loop fingerprints.

Loops pattern can be found in 60%–70% of all encountered fingerprint patterns [14]. In the loop pattern, at least one ridgegoes inside of the imprint, re-curves or intersect the line joining from the delta to the core and end the direction at the side where the ridges started. It has at least one core, one delta and a ridge count for every loop pattern [15]. Radial loop pattern is a concentric pattern, the pattern is sloped towards the radial bone, the thick bone of the thumb side. The direction of the radial loops is like the radius leading towards the thumb. It is rare to find these radial loops. But, in generally, we can find it on the index fingers. Ulnar loop is the most common pattern. Sometimes, it is also similar to the radial loop but sloped towards the small bone of the arm, the ulna, on the same side as the little finger. Examples of the arch fingerprint pattern and the loop fingerprint patterns are shown in Figs. 2 and 3.

(3) Whorl fingerprints.

Whorls can be found in about 25%–35% from all encountered fingerprint patterns [16,17]. Some ridges turn through at least one

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

(a) Radial Loop

(b) Ulnar Loop

Fig. 3. Loop fingerprint patterns.

(a) Core and Delta

(b) Fingerprint structure

Fig. 5. Examples of the Ridge characteristics on the finger.

circuit. Every pattern of fingerprint containing at least two deltas can be the whorl pattern. Normally, we can find whorl patterns in four types. These four types are summarized in the following.

1. Central pocket loop whorls
   In this pattern, the ridges create one complete circuit. That circuit can be spiral, oval or any types of a circle. There is one or more re-curving ridge or an obstacle at the right angles with the flow line. Example of central pocket whorl is shown in Fig. 4(a).
2. Plain whorls
   The ridges are turning to make one complete circuit with two deltas. Therefore, the plain whorls are circular or spiral in shape. Example of plain whorl pattern is shown in Fig. 4(b).
3. Accidental whorls
   In accidental whorls, it has two patterns and also two or more deltas. The patterns of accidental whorls are not the same. The ridges match the characteristics of a particular whorl sub-grouping. Example of whorl pattern is shown in Fig. 4(c).
4. Double loop whorls
   This pattern consists of two distinct and separate loop creations. For every core, it consists of shoulder and two deltas. A complete circuit is created with one or more ridges. Example of double loop whorl is shown in Fig. 4(d).

2.1.2. Fingerprint structures

In a family, fingerprints general patterns could be the same in level one. But they are different in level two and three because they are not inherited [18,19]. As soon as the formation processing finished of the fingerprints, they grow the ridges uniformly in all directions during their growth process. This is the reason that the pattern had never been changed. They never change even if the skin tissue is torn, it grows back as the same print before. Therefore, fingerprints endured the same throughout our lives.

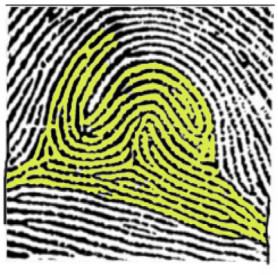
As fingerprint is made up of ridge characteristics, ridge characteristics is included in an important session in the explanation of fingerprint [20]. Ridge characteristics are the points that can be used for recognition purposes. Typically, an enrolled fingerprint may include more than 100 recognition points. There are many different ridge characteristics. For a positive recognition, it needs to make comparison for a variety of points depending on the frequency of the ridge characteristics.

The overview of the fingerprints structure is shown in Fig. 5(a) and 5(b). Fig. 5(b) shows some examples of the ridge characteristics. The details structure of the ridge types are shown in Figs. 6 and 7. Generally, there are 16 types of the fingerprint's ridges. They are:

1. Ridge: Ridge is the very basic pattern of the fingerprint and it can be any pattern of the fingerprint.
2. Core Ridge: It is located in the fingerprint center area. In a fingerprint, there may be more than one core or no core. It determines the fingerprint type such as a whorl, loop or arch pattern. Examples of core are shown in Fig. 6(p).
3. Delta Ridge: It is similar to the Greek letter δ, and is shown in Fig. 6(l).
4. Enclosures (Lake): The ridge pattern is like the lake. Firstly, it will separate from one ridge and at the end, it will merge into one ridge again. It has been shown in Fig. 6(h).
5. Enclosures Ridge: Enclosure ridge is a ridge where ridge dots or the short ridge has been enclosed as a compound. Examples of such enclosures are shown in Fig. 6(n).
6. Loop Ridge: The ridge has a bending shape pattern curving around itself. It is illustrated in Fig. 6(p).
7. Ridge dots: It is a small isolated pattern where the length and width are approximately the same. It is shown in Fig. 6(a).
8. Ridge crossing: The two ridges are crossing and intersect with each other. It is shown in Fig. 6(g).
9. Short Ridge (Islands): The pattern looks like an island in the middle of two other ridges. It is shown in Fig. 6(i).

(a) Central Pocket Whorl

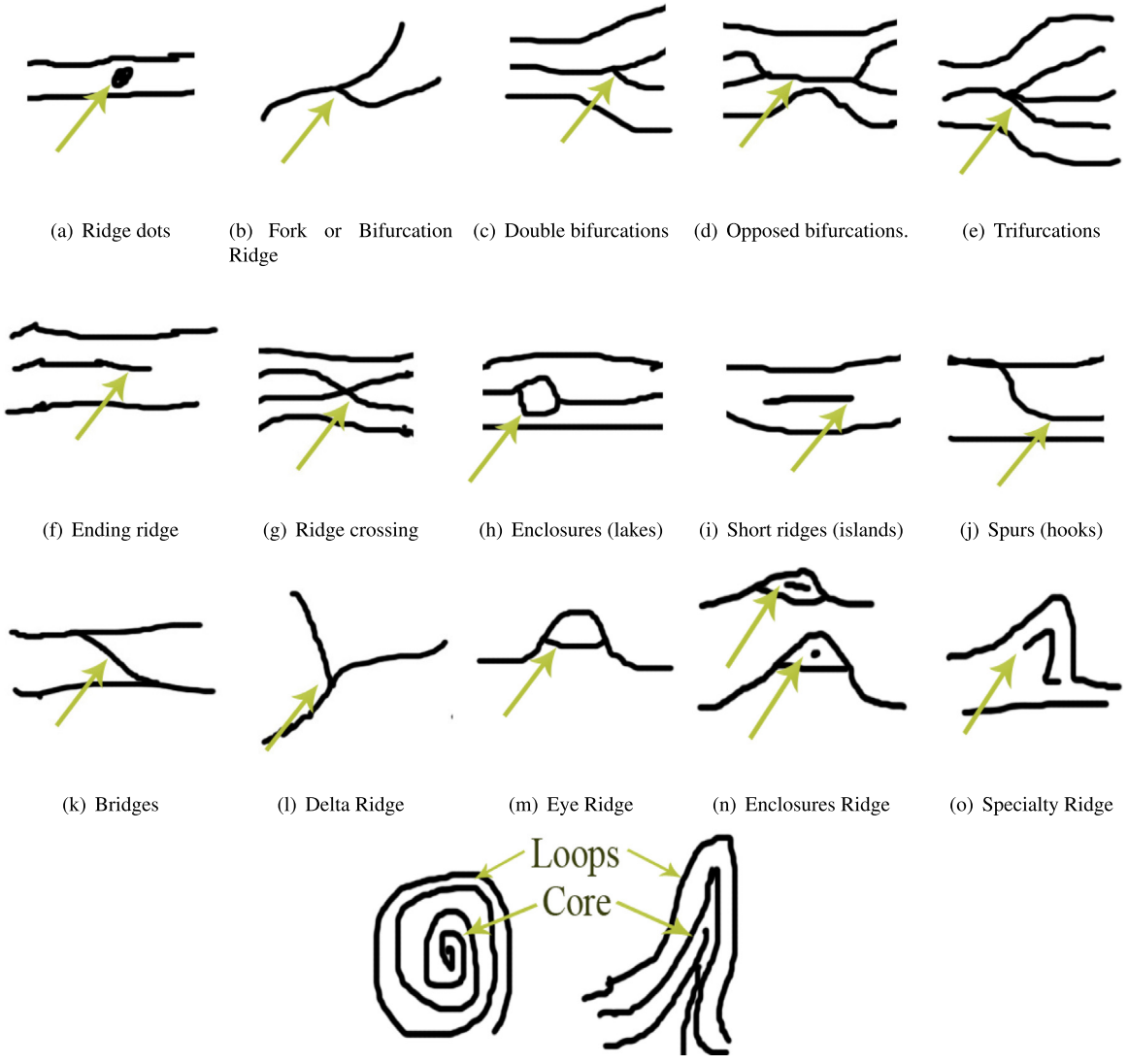
(b) Plain Whorl



(c) Accidental Whorl

(d) Double Loop Whorl

Fig. 4. Whorl fingerprint patterns.



(a) Ridge dots (b) Fork or Bifurcation Ridge (c) Double bifurcations (d) Opposed bifurcations. (e) Trifurcations

(f) Ending ridge (g) Ridge crossing (h) Enclosures (lakes) (i) Short ridges (islands) (j) Spurs (hooks)

(k) Bridges (l) Delta Ridge (m) Eye Ridge (n) Enclosures Ridge (o) Specialty Ridge

(p) Core and Loops Ridge

Fig. 6. Different types of ridge characteristics.

10. Eye Ridge: The shape of the pattern looks like an eye. It has been shown in Fig. 6(m).
11. Specialty Ridge: The shape is very different from usual ridge patterns, and it is thus called specialty ridge. It is shown in Fig. 6(o).
12. Fork or Bifurcation: There are two kinds of bifurcations: double bifurcations and opposed bifurcations. Examples of bifurcation ridges are shown in Fig. 6(b), 6(c) and 6(d). Fig. 6(b) is a general bifurcation ridge. Fig. 6(c) is a double bifurcations ridge in which the ridge is double and Fig. 6(d) the opposed bifurcation ridge in which the double ridges are opposing one another.
13. Trifurcation: A trifurcation ridge is a ridge that is separated into three ridges as shown in Fig. 6(e).
14. Ridge Ending: Ridge Ending is the termination of a ridge. It is shown in Fig. 6(f).
15. Spurs(hooks): A spur ridge is a ridge pattern having a hook-like shape. It is shown in Fig. 6(j).
16. Bridges: A bridge ridge is a ridge connecting two ridges like a bridge. An example is shown in Fig. 6(k).

2.1.3. Unusual fingerprints

Some fingerprints can be existed as unusual fingerprint such as Psoriasis and scar tissues [21]. Psoriasis can be formed based on the chronic skin condition because the overactive immune system. This kind of psoriasis are flaking, inflammation, thick, white, red patches of the skin. It also can be cured by applying steroid creams and occlusion and light therapy. In the ancient Greek, it has been named as Psoriasis. Usually, this Psoriasis can be found on the scalp, elbows, knees and lower back [22]. And another unusual fingerprint is formed because of scar tissues. The unusual fingerprints are shown in Fig. 7.

2.2. Fingerprint in criminal investigation

Fingerprint is one of the essential forensic techniques in the analyzing of the criminal evidence because of its uniqueness and persistence. Not only fingerprint, blood, DNA, handwriting, hair, fibers, foot prints are very useful in the investigation of the crime scene. Among them, fingerprint have been used for centuries in criminal Investigation in order to identify the person whether it can be the suspects, the victims or the witness, etc. [23]. When the crime scene examiner discovered the print from the crime scene, they collected the print and made analysis in very

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

(a) Psoriasis (b) Fragmenting (c) Scar tissue

Fig. 7. Unusual types of fingerprints. (a) Psoriasis, (b) Fragmenting: fragmenting is formed in the center, (c) Scar tissue: the scar may creates a new unique print.

detail, and then they reported the analysis results to the law enforcement.

2.2.1. Collection of the print

To collect prints, it is important to consider the surface of the investigation scene to decide which collection methods should be employed. Regularly, the surface can be absorptive surface, non-absorptive smooth surface and non-absorptive rough surface [24,25]. The difference between absorptive and non-absorptive surfaces is whether they are able to absorb liquids or not. Table 1 shows the powder type for fingerprint extraction and the type of materials area for criminal investigation [22].

The absorptive surfaces are the surfaces such as paper, cardboard, and untreated wood [26]. And some chemicals such as ninhydrin can be used by scattering it on the surface and then the photograph can be taken for this developing fingerprint. Non-absorptive smooth surfaces are the surfaces that have been varnished or painted, and plastics, glass. For the collection on this non-absorptive smooth surface, the analyst uses powder-and-brush techniques and then the print is lifted using tape. Non-absorptive rough surfaces are the surfaces such as vinyl, leather, and other textured surfaces. In this rough surface, the expert not only apply powdering process but also use something to get the print from the surface grooves such as gel-lifter, silicone casting material etc.

Because there are three types of fingerprints, the collecting methods will be varied depending on the fingerprint type. To collect latent fingerprint, it is made from the sweat and oil of our body skin. It is required to apply some other process for the visibility of the print such as basic powder techniques or some other chemicals [27]. And also, for the collection of the patent fingerprints, it can be acquired by using blood, grease, ink or dirt. It can also be seen easily. For the collection of the plastic fingerprint, it can get by pressing the fingers into some soft materials such as the fresh paint, wax, soap etc. Usually, the print that can be found in the scene are latent fingerprint.

2.2.2. Analysis of fingerprints

After they collected the prints from the crime scene, the analysis process is started. In other words, it can be seen as comparing unknown print which is collected from the crime scenes with the known print that is stored in the database [28]. During this fingerprint analysis process, if the collected fingerprint is not clear, accurate and complete, it can create the problems in the fingerprint recognition process [29]. Because of this reason, the fingerprint examiners decide whether there is enough information in the print to be used for recognition or not. The analysis includes determining class characteristics and individual characteristics by comparing one point by one point until they have found the possibility of the match for the collected unknown print.

In class characteristics, there are three class: arches, loops, and whorls [30,31]. The collected print is specific into one of these three group by analyzing. After grouping, it again narrows down to individual characteristics. Individual characteristics are the unique characteristics for every personre17. They are very tiny irregularities among fingerprints that come out within the friction ridges. They are also known as Galton details, points of identity, or minutiae. They consist of three basic types: ridge endings, bifurcations (a ridge that divides) and dots. Recognition of the fingerprints relied on the pattern matching by detecting of certain ridge characteristics [32]. If they find any unexplained differences between these two fingerprints, they exclude the known fingerprint as the source from the database. In other way, if the class characteristics are not the same, the conclusion would be exclusion. If the fist characteristics and the individual characteristics are the same between the two fingerprints, the conclusion would be recognition.

In some cases, there may not be any of these two conclusions [33,34]. In such case, it is because there may not be enough ridge detail to make comparison effectively. It is named as inconclusive. Therefore, there are three potential outcomes that can be available from a fingerprint examination: exclusion, recognition and inconclusive. After the first fingerprint examiner finish the examination, another examiner repeats the process again independently. And if both of the examiners agree and the results are the same, the fingerprint evidence becomes strong evidence and it is reported to court. The fingerprint examiner records each and every details of the recognition process and keeps the complete documents, make report and do the conclusions. And if the law enforcement used the fingerprint in the trial, these records needs to testify by the examiner about the process in the court. Fingerprint recognition techniques are developed accompanying by the technology and the forensic science is also essential for years.

Fingerprint can even express the routine, lifestyles, action and story of our entire lives such as what we have been used and what we have been consumed by looking the molecules on the fingerprint using mass spectrometry technology [35,36]. We can even say fingerprint as story teller. So, it is one of the most effective and essential technique in searching the evidence and proof in criminal investigation.

As one of the examples of the application scenarios, it has been surveyed for three year concerned with the offenses of residential burglary, commercial burglary and motor vehicle's theft. For these three crime types under, in 11,781 crime scenes, fingerprints were found and this created 1942 fingerprint recognition. The recognition of 653 were successful and transformed into detection. Mostly fifty percent of fingerprint recognition is achieved during thirteen days of the crime and ninety percent of recognition is achieved within thirty four days from the crime being reported [37].

As crimes have been increasing along the time and according with these growing crimes, Fingerprinting has been essential

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

Table 1
Powder types and their application areas.

Powder	Materials
Pure gray powder	General materials
Black powder	Paper, unglazed pottery, eggshells, synthetic resins
White powder	Leather, rubber, oily fingerprints
Copper powder	Plant stem and leaves, fruit rinds
Gold powder	Rough surface metals, synthetic resins
Yellow power	Leather, rubber
Lycopodium powder	General materials, oily fingerprints
Dragon blood powder	Rough surface metals, stone
Indigo powder	Synthetic resins, frosted glass, metal frames, eggshell
SP Black Powder	Aluminum building materials
Ultranium powder	Synthetic resins
Aluminum powder	Glass, ceramics, lacquer
Pure aluminum powder	Synthetic resins, plated metal
Lead carbonate powder	Synthetic resins, leather
Stone powder	Leather, rubber, oily fingerprints
Fluorescence powder	Color print paper (viewed under UV light)
Anthracene powder	Leather, rubber
Magnetic powder	Paper (works with brush or wand)

tool for investigating officers. If fingerprints can be distinguished according to gender, the workload would be reduced to the extent of half for the officers. In [38], Nayak et al. studied about density of the fingerprint based on the gender for revealing the differences of the sex characteristics in the density of the fingerprint ridge. Esperanza et al. discussed the fingerprint density uncertainty to determine the differences by counting epidermal ridges from the Spanish population [39]. The experimental results showed that female have obviously greater ridge density than men for all ten fingers in the area of radial and ulnar count. In [40], Acree also studied about the density for the ridge between men and women by conducting Caucasian and African American descent and they proved that women are likely to have significantly higher ridge density than men regardless of race.

2.2.3. Fingerprint recognition system

Fingerprint recognition is very popular because of its success in the variety of applications such as government, forensic and civilian domains [14,16]. The availability of large legacy databases, condensed and economical fingerprint readers enhanced the popularity of the fingerprint. Fingerprint recognition system is used for both verification and recognition purpose. In verification, the enrolled finger is compared with the identified user to conclude if the two prints are from one finger as (1:1) matching. In recognition, the input fingerprint is compared with all of the database enrolled prints for determining if that one has already been realized under an identical as (1: N) matching.

The Integrated Automated Fingerprint Identification System (IAFIS) is another greatest fingerprint recognition system and is maintained by Federal Bureau of Investigation (FBI) in the United State since 1999 [19,40]. In the system, there are abundance of fingerprint cards and the criminal history documents proposed by law enforcement agencies. It provides not only searching 10-print ID for suspect recognition, latent print for criminal investigation but also general population for the person's background checking. It is also used for assisting fingerprint examiners for their examinations. The system was allowed for accessing the national fingerprint repository in Clarksburg, West Virginia for FBI and other criminal justice agencies for tracking with fingerprint throughout the United states. It may be recorded for the individuals who are arrested in the FBI criminal master file (CMF). And after that, it may also include for the fingerprints that is need to be fingerprinted as a part of a background checking for some works like military service as FBI civil file (CVL) [18]. Nowadays, FBI has been updated the IAFIS to another version called Next Generation Identification (NGI) system. The updated system provides not only for the fingerprints but also for bio-metric traits such as palm print, iris and face [2].

Not only for the investigation of the crimes, the Automatic Fingerprint Identification System (AFIS) and fingerprint can be used as the recognition of the dead person. The reason of using fingerprints is cost-effective and the results report can get rapidly. As an example, in the disaster situations, the death of the bodies cannot be identified easily. And for the recognition, the prints may have been recorded from airline manifest and in the system. The record can be compared with discovered postmortem impression based on the number of fatalities manually. To compare with the system, firstly, the postmortem examination prints are scanned into the system and digitized the friction ridge characteristics and minutiae.

As an example of the best addressing of the AFIS deployment and the fingerprints usage for big fatality victim recognition, there was a huge tsunami that has been taken placed in the coastal of Thailand on December 26, 2004. It had been killed more than five thousand people. In the accordance with that Thailand is one of the very famous tourist attractive countries around the world, the dead were both a lot of local citizen but also many visitors all over the world especially from northern Europe such as Denmark, Norway, and Sweden [18]. It has been requested from a worldwide for the antemortem recognition records. For that reason, AFIS was denoted to help in this recognition because there did not exist automated fingerprint system in Thailand. Fingerprints offered by many different government agencies, latent prints collected on items and also taken prints from the dead, were submitted into AFIS and used as antemortem standards [18].

Additionally, to give an instance of the usage of fingerprint in daily life, the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program of the US Department of Homeland Security is deploying fingerprint recognition technology in the issuing posts of the visa and entry port. With the help of this deployment, the federal government can verify the identity of the visiting person to the United State. Since 2004, it has been operated more than 100 million visitors. Therefore, the system is helping in identification of not only the terrorists and criminal person but also the immigration violators. This is done by comparing the fingerprints of visa applicants and the fingerprints from the watch-list database. Moreover, the system can also verify that a foreigner at the entry port is the same with the person whom the visa was delivered [41]. Similar to the US, some of the international airports from Japan and other countries are also taking foreigners fingerprints and photos for the recognition of the person.

Generally, there are about 20–70 minutiae points in a standard fingerprint image, and it depends on both the surface of the fingerprint sensor and the way users place their finger on the

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

sensor. And then, the minutiae direction and location information are stored in the system with the demographic information of the user in the database. In the recognition phase, the user impresses the sensor utilized for the enrollment by creating a new fingerprint image as the query print. The system extract minutiae points from the inquiry print and the matching module of the system analyzes the inquiry minutiae set to calculate the number of common minutiae points with the fingerprint in the database. Before the matching process starts, the minutiae points taken from the template and the inquiry fingerprints must be adjusted and registered because of the pressure and the variation of the finger placement on the sensor. After these adjustments, the matching module assesses the similarities in terms of location and directions for the two prints. Subsequently, the system determines the identity of the user based on a match score and a threshold set by the system authority.

The classical fingerprinting approach of using ink and paper is also utilized by some law enforcement agencies. For the creation of ink fingerprinting, firstly the person finger is cleaned to remove sweat and other dusts. After that, ink is applied to the finger surface, which is then rolled onto the prepared cards from one side of the fingernail to another. This is called rolled fingerprint. Finally, the card is scanned to generate a digital print image. In law enforcement, a typical fingerprint image resolution is 500 pixels per inch (ppi). Sometimes, law enforcement uses larger sensing surfaces such as 10 print scanner to take palm prints and all four fingers at the same time. As for commercial applications, low-resolution and small readers are more suitable for easy embedding in consumer devices such as laptop touch sensors, mobile phones and PDAs.

As for open source fingerprint readers, Engelsma et al. proposed the Raspi Reader that is an open source fingerprint reader for fingerprint matching and assisting in detecting spoof fingerprints [42]. They also proposed an open source design of a high resolution, spoof resistant, optical fingerprint reader [42], called"RaspiReader". The reader can detect spoof fingerprints by using two cameras for capturing fingerprint images.

3. Fingerprint classification and recognition algorithms

In this section, we discuss fingerprint recognition, fingerprint classification, fingerprint matching, feature extraction and Finger-Vein recognition concerning with the machine learning algorithms applying for fingerprint classification [5,6,26,43]. And fingerprint spoof detection is also explained at the end of the section. Fingerprint recognition is to identify unknown fingerprint and name the fingerprint. Fingerprint classification is the classification of the fingerprints into a category or a group. As a consequence, we present fingerprint recognition and classification separately. As an example, the thinned fingerprint, the classified fingerprint that has been transformed into the binary are demonstrated in Figs. 8 and 9.

Fingerprint Thinning is very important in the classification of the fingerprint as the pre-processing of the classification. Thinning is the process of obtaining the skeleton of the image and removing all redundant pixels to get a new clarified image. The skeleton can be as a line thicken as one pixel and can show the topology of the image. Concerning with the fingerprint thinning, Bin Fang. et al. proposed a fingerprint thinning algorithm based on the directional image [44]. And also, Luping et al. proposed an algorithm for binary fingerprint image thinning and other common images with a template-based pulse-coupled neural-network model [45]. And also, Espinosa-Duro presented fingerprint thinning algorithm using morphological image processing operation [46]. Khanyile et al. discussed the fingerprint thinning algorithms extensively in [47]. They exclusively studied and compared about the thinning algorithms. According to [47], there are two main approaches in thinning algorithms, i.e., iterative boundary removal algorithms and non-iterative distance transformation algorithms. In iterative approach, it removes the boundary pixels of a pattern continuously in the expectation of remaining only unit pixel-width thinned image and contains sequential and parallel algorithms. In non-iterative approach, it is not as robust as iterative approach and are not suitable the applications and contains Medial Axis Transforms and other [47]. And also, the process of the transformation steps for the thinned fingerprint has been presented and discussed in [47–49].

Every fingerprint classification algorithm has its own advantages and disadvantages. Fig. 10 shows the summary of fingerprint classification algorithms, the techniques to support for the fingerprint's enhancement, and spoof fingerprint detection.

3.1. Fingerprint classification

Fingerprint classification has been developed from the start of computer invention. As a classification method, Henry's classification method is the most widely used classification method for fingerprint. The method has been evolved to the AFIS. It is based on the eight classification of the prints (namely plain arch, right loop, tented arch, plain whorl, left loop, double loop whorl, central-pocket whorl and accidental whorl).

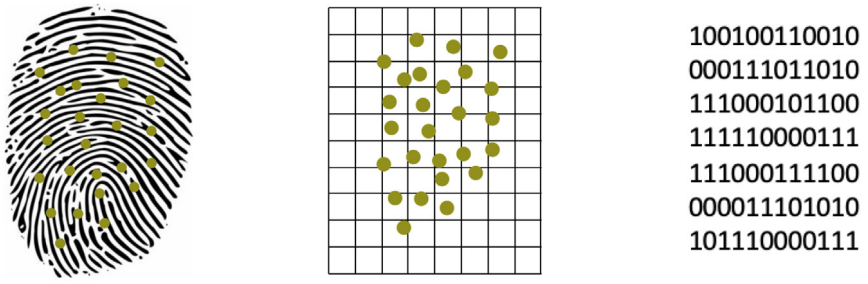
3.1.1. Based on deep learning/ neural network

Some machine learning, deep learning methods have also been used for the building of the fingerprint classification algorithm: fuzzy and Back Propagation Neural Network algorithms. Based on depth neural network, Wang et al. proposed a fingerprint classification algorithm [5]. They adopted the softmax regression for fuzzy classification for the improvement of the classification accuracy. They provide a secondary class for the "suspicious" fingerprints. In [20], Kamijo proposed a two-step learning method as the learning process together with the four-layered neural network, and applied in classifying fingerprint images and deriving the classification state. In [21], Mohamed et al. presented a fingerprint classification system and its performance in an recognition system depending on the extracting of the fingerprint features. They used fuzzy-neural network classifier for classifying of the input feature codes according to Henry system. In the proposed system, it includes four steps, segmentation, directional image estimation, singular point extraction and feature encoding. It includes the singular points (core and delta) encoding with directions and positions. Kouamo et al. proposed a model for the authentication of the people by fingerprints using neural network having a multilayer perceptron structure and extraction algorithm [16]. They used the calculation of probabilities for the classification of the input image sub-blocks. In [7], Ala et al. proposed a method for the dimension reduction of the feature's vectors for characterizing fingerprint. And they evaluated their method using Back Propagation Neural Network (BPNN). In [19], Baldi et al. designed a neural network algorithm for the recognition of the fingerprint. They introduced a couple of fingerprint images and the algorithm estimating the probability of the two images from one finger. Singular Points are important for representing local ridge pattern characteristics and for determining the topological structure.

3.1.2. Based on SVM, K-means, Apriori

And also, many research have been done for the fingerprint classification algorithm relying on the Support Vector Machine (SVM), K-means classifier, clustering and Apriori algorithms. In [8], Yao et al. proposed a machine learning approach depending on SVMs and Recurrent Neural Networks (RNNs) for the classification. They train RNNs for the structured representation of the

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.



(a) Minutiae Point of Fingerprint (b) Fingerprint Minutiae (c) Fingerprint Minutiae with Binary Code format

Fig. 8. Taking minutiae point of fingerprint for the classification process.

(a) Original Fingerprint (b) After processing (c) Thinned Fingerprint

Fig. 9. The process of getting thinned fingerprint.

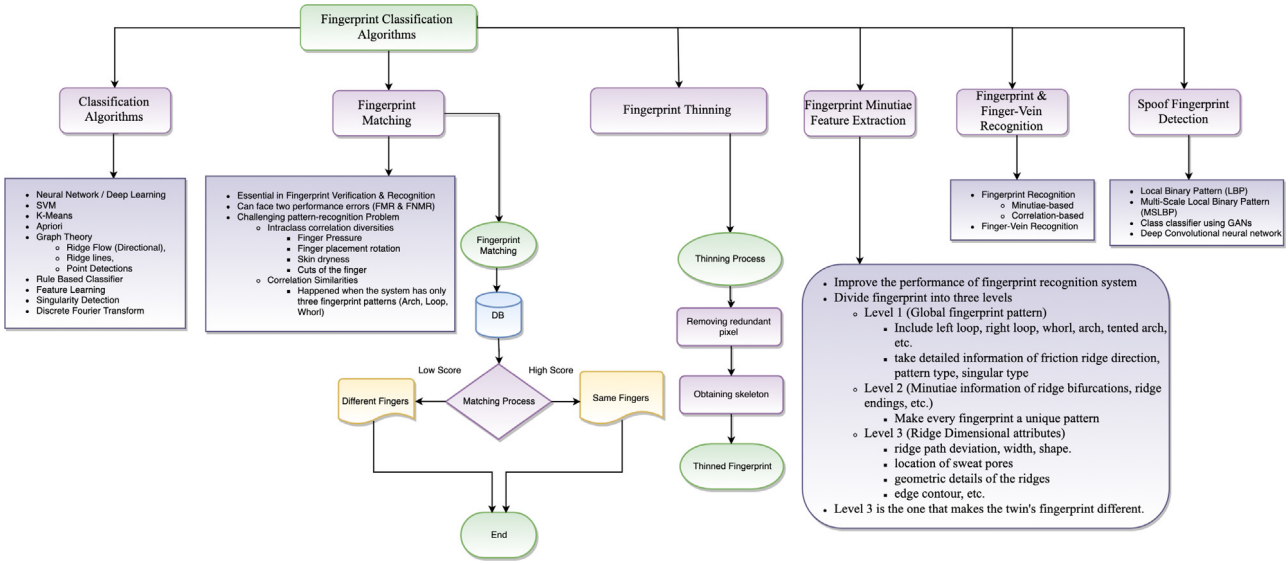


Fig. 10. Fingerprint classifications algorithms and its fingerprint enhancement techniques.

fingerprint image and use it to extract a set of the distributed features to integrate in the SVMs. They combined SVMs with a new error correcting code scheme. In [28], Ji et al. presented a classification method depending on orientation field and support vector machines. The method can estimate orientation field from pixel gradient and then they calculate the ratios of the direction block classes. Li et al.. proposed an algorithm based on the interactive validation of singular points and the constrained nonlinear orientation model [29]. They also used SVM classifier to perform classification for input of the compact feature vector. In [23], Wang et al. proposed fingerprint classification algorithm based on directional fields. They calculated fingerprint image directional fields and discover singular points (cores) and then they extract features. They used k-means classifier and 3-nearest neighbor for the classification of the features and fingerprint patterns (arch, loop and whorl). For the generating of the numeric code sequence, Bhuyan et al. proposed an efficient classification fingerprint technique using data mining approach for every fingerprint image depending on the ridge flow patterns [34]. They used Apriori algorithm for frequent itemsets generation technique to select a seed for each class. And then, K-means clustering is used to cluster the seeds for the fingerprint images.

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

3.1.3. Based on graph theory, directional, ridge flow, ridgelines, point detection

In addition, some researches have been based on the graph theory, directional ridge flow, ridgelines and point detection methods for the fingerprint classification. By using graph theory, Tarjoman et al. introduced a new structural approach for the fingerprint classification applying fingerprints directional image [35]. They segmented fingerprint directional images into pixels regions with the same direction. In [50], a fingerprint recognition algorithm was proposed based on core analysis for core point candidate's detection from the directional fingerprint image and to analyze the near area of each core candidate. The core point orientation is extracted for the classification step and unclear core points are eliminated. Using the Sobel operator and Gabor filter, Nain et al. proposed an algorithm depending on ridge-flow patterns tracing by extracting the High Ridge Curvature (HRC) region [31]. In [51], Liu et al. proposed an algorithm relying on changing the ridgelines total direction (the ridgelines curve features) for classifying the ridgelines. Using signum change, Ramo et al. proposed a singular point detection algorithm for core and delta points curves in the directional images [25]. The proposed algorithm is able for detecting all the actual singular points with accurate precision with high speed. In [30], Zhou et al. analyzed singular Points and proposed an algorithm for singular point detection depending on the global orientation field. They used core–delta relations as a global constraint for the final decision.

3.1.4. Based on rule based classifier, feature learning, singularity detection and discrete fourier transform

Furthermore, other researches are based on rule-based classifier, feature learning, singularity detection and Discrete Fourier Transform (DFT). Some rule-based methods are relying on the global ridge features or the singularity features, but in some cases, based on both of these methods [36]. Based on the rule-based classifier, a new fingerprint classification algorithm has been proposed to extract singular points from the fingerprint image and to classify depending on the detected singular points locations and number [43].

Karu et al. classified fingerprints into five categories: arch, tented arch, left loop, right loop and whorl in that paper. The rules are generated independently form a given data set. Tan et al. presented a fingerprint classification approach depending on a novel feature-learning algorithm [24]. Their method relied on Genetic Programming (GP) for discovering the composite features and operators. In [33], Liu et al. proposed an improved rapid classification algorithm using singularities detection to classify the fingerprint into 5 classes and to increase the accuracy. He also use the delta direction and singularities to partition the similar classes. In [26], Park et al. presented an approach for fingerprint classification based on nonlinear discriminant analysis and DFT. Firstly, they used DFT and directional filters to construct an efficient and reliable directional image from every single fingerprint image. After that, for building directional images, they used nonlinear discriminant analysis by extracting the discriminant features and decreasing the dimension.

While many researchers have focused on the classification of the fingerprint, Kant et al. presented an approach to accelerating the matching process and decreasing the processing time by classifying the fingerprint pattern into different groups at the enrollment process of the fingerprint recognition system [52]. And they improved fingerprint matching while matching the input template with stored template. Moreover, Si et al. proposed a method for the distorted fingerprint in the purpose of the detection and rectification. They implemented distortion detection as a two-class classification problem. The registered ridge orientation map is used as feature vector and then after that, SVM classifier is used for the classification task [11]. In [12], Gu et al. also presented a method for the rectification of the distorted fingerprints depending on a single fingerprint image with faster performance. They used Hough-forest-based two-step fingerprint pose estimation algorithm and support vector regressor-based fingerprint distortion field estimation algorithm.

3.2. Fingerprint matching

Fingerprint matching is the process of matching the similarity score between the two fingerprints. The score will be relatively high if the two prints are from the same fingers, and it will be comparatively deficient if the two prints are not from the same fingers respectively. The process of fingerprint matching is a challenging pattern-recognition problem because of its intraclass correlation diversities from the fingerprint images of the same finger and its correlation similarities from the fingerprint images of different fingers. This type of diversities occurs especially because of the finger pressure, finger placement-rotation and the skin dryness and cuts of the finger etc. For the type of correlation similarities, it happens exclusively when the system defines the print only for three fingerprint patterns type (arch, loop and whorl).

The method of decomposing minutiae-based fingerprint matching for the big data framework was proposed in [53]. In that framework, they proposed a generic decomposition methodology for minutiae-based matching algorithm. It split the scores of the matching into very detail processes. By decomposition, any minutiae-based algorithm can be adaptable to the frameworks such as MapReduce or Apache Spark [53]. In [54], Lee et al. proposed a new partial fingerprint-matching using minutiae and Ridge Shape Features (RSFs) for all sensors in mobile devices. RSFs is the small ridge segments where specific edge shapes are observed. A novel dense fingerprint registration algorithm was proposed in [55]. It includes a composite initial registration process and a dual-resolution block-based registration process.

Concerned with fingerprint matching performance, there can be two kinds of errors that can occur. They are a false match (the output shows that the print is matched from two different fingerprint images) and a false non-match (it cannot match and identify the image from the same finger). This False Match Rate (FMR) and False Non-Match Rate (FNMR) are influenced by the operating threshold. If threshold score becomes more, it can occur less FMR and vice visa. And it is difficult to reduce both of these errors at the same time [2]. Some examples of the difficulties types that can be faced in the fingerprint matching process are because of the skin condition (wet skin, etc.), image noise (fingerprint with many cuts), overlapping latent fingerprint, modified fingerprint (some criminals alter his fingers with Z-shaped incision), distortions, rotations and displacement of the fingerprint.

This fingerprint matching is also an essential process in both fingerprint verification and fingerprint recognition problems. In general, the algorithm of fingerprint matching compares the two fingerprints and output the similarity rate (a real number bounded into an interval) or a dichotomic output (matched or not matched) [56]. The results of the comparison can be in two situations: genuine if the prints are from the same finger and impostor if they are not from the same finger.

3.3. Fingerprint feature extraction

Feature extraction algorithm influences the performance of modern automated fingerprint recognition systems. We can divide the patterns of fingerprint into three levels for feature extraction. Level 1 presents global fingerprint patterns (overall fingerprint ridge flow). In level 1, it includes five categories (left

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

loop, right loop, whorl, arch and tented arch). It take details information of friction ridge direction, pattern type and singular points. Global ridge flow is a well-defined pattern and can be extracted easily even though the quality of the image quality is deficient [14]. The next level features are relevant with minutiae information of ridge bifurcations and ridge endings, etc. And it made every fingerprint unique pattern. Ridge ending such as bifurcation are used in defining level-2 features. In the next level (level 3) features, it consists of ridge dimensional attributes (ridge path deviation, width, shape, the locations of sweat pores, geometric details of the ridges, edge contour) and also other details such scars, incipient ridges, etc. It needs to use microscope and this level is especially used in forensic examiners. The differences between identical twins start in level 3. It is needed to be high resolution image to get more higher-level features. For instance, to extract the features from level 3, it requires the image with the resolution of more than 500 ppi. Using artificial neural network, Pavol et al. proposed fingerprint recognition system to detect the important image regions based on level 2 features [14].

Galar et al. extensively and explicitly studied about the methods of feature extraction and its learning models [57]. They considered fingerprint classification from two perspective of the learning models and feature extraction. And they also presented singular point detection, orientation map extraction and feature extraction. In [58], Michelsanti et al. proposed an approach that do feature extraction with fast speed and that will not need heavy pre-processing stage. It uses pre-trained CNNs and Visual Geometry Group-Face models such as (VGG-F and VGG-S) to address fingerprint classification problem. VGG-S and VGG-F are the pretrained model architecture of CNNs. By using mobile device camera, Barra et al. proposed an entire architecture for a mobile hand recognition system to acquire the hand in visible light spectrum [59]. They made contribution in two perspective. The first one is to investigate the dimensionality reduction methods for the identification of the features subsets containing the most discriminating and robust ones. And the another one is for comparing the matching strategies.

As a general typical minutiae feature extraction, Anil K. et al. have described how to extract the feature from a fingerprint [2]. They firstly estimated the ridge orientation direction and density of the image. Depending on this assessment, they implement the contextual filtering for the improvement of the image quality and for the facilitation of the ridges extraction. From the enhanced image, it can be achieved the binary ridge skeletons by following of ridge endings and ridge lines. Afterwards, bifurcation points will be available from this ridge skeleton as minutiae. For the detection and removing of the spurious minutiae getting from the incomplete skeleton image, some heuristic rules can be applied [2].

3.4. Fingerprint and finger-vein recognition

3.4.1. Fingerprint recognition

For the improvement of the fingerprint recognition system performance, it is measured with False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR) [2]. FPIR occurs if the system finds the print that is not enrolled into the system. And FNIR occurs if the system cannot show the print that has already enrolled into the system or show the wrong print. The relationship between FPIR and FMR can be defined as $FPIR = 1 - (1 - FMR)^N$, where N is defined as the number of the user enrolled into the system. Therefore, the number of the registered users increased, FMR needs to be decreased.

For the effective recognition, the two fingerprints must have the same general pattern. It needs to be some common ridge characteristics for both fingerprints. The common ridges can be varied based on the availability of the prints and the similarities of the characteristics. Generally, there are two methods for fingerprint recognition, minutiae-based techniques and correlation-based techniques.

- Minutiae-based technique: It finds the points of the minutiae. Afterwards, in order to match the ridge characteristics, it maps their relative placement on the finger. But it can be challenging for extracting the minutiae points accurately especially when the prints are not clear enough for the matching. And it does not consider the global pattern of ridges.
- Correlation-based technique: This method can solve some challenging tasks of the minutiae-based approach. However, it also needs to get the precise location of the registration point and it can be influenced by image translation and rotation.

According to our survey, it needs to make the quality of the fingerprint image to improve the accuracy of fingerprints recognition by AFIS. In [60], Ding et al. designed a novel fingerprint enhancement filter named 2D Adaptive Chebyshev Band-pass Filter (ACBF) with orientation-selective. It includes two stages in this filter. Firstly, the fingerprint quality can be increased using Gabor filter and Histogram Equalization (HE) and then it is enhanced again based on spectra diffusion using the 2D ACBF with orientation-selective in frequency domain. With this improved quality of the fingerprint, the performance of the automatic fingerprint recognition system is improved. The holes and gaps in the ridge can be filled by the standard fingerprint enhancement methods such as Gabor and anisotropic filters. But for the scar, the gaps and holes among the ridge cannot be filled. For this reason, Khan et al. proposed a method to enhance the fingerprint image by removing of the scar [61]. They use the Fourier domain directional field for the suitable candidate of the scar pixels to be replaced.

It is required to process millions of fingerprints per second so that it can implement an abundance of minutiae per second. As a result of this requirement, Miguel et al. proposed a new minutiae design based on fingerprint matching algorithm with Graphics Processing Unit (GPU) based parallel architectures [62]. It can implement several GPUs in parallel and fingerprint processing rates from 300,000 to 1,500,000 fingerprints per second. In [63], Raffaele et al. presented a new parallel algorithm for the performance enhancement of the fingerprint recognition using GPUs. It enables a medium-scale AFIS to run on a standalone PC with four Tesla C2075 GPUs.

Additionally, a flexible dual phase recognition method has been proposed and it is named as a Dual Phase Distributed scheme with Double Fingerprint Fusion (DPD-DFF) for accurate and fast recognition in large databases [64]. It performs by the combination of two matches and two fingers inside the scheme of hybrid fusion to get the high speed performance and improve the accuracy. In [65], Miguel et al. proposed a clustering algorithm for the self-reliant of the minutiae descriptors. Their technique increased the robustness of recognition in the large non-linear deformation for latent fingerprint images. Daniel et al. proposed a hierarchical classification framework for a complete recognition system [66]. That framework combines the information of multiple feature extractors. They adopted feature selection in the system for the accuracy improvement of the classification. The distributed recognition system is implemented by applying the incremental search to discover the classes consistent with the probability given by the classifier. There is a single parameter to tune the trade-off between recognition time and the accuracy [66]. For the deployment of k-means clustering algorithm, it has been proposed a novel fingerprint indexing algorithm based

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

on minutiae details and convex core point. It also based on the triangles and their deep relations to ellipses. They also employed candidate list reduction criteria to improve the performance of the indexing algorithm [67].

3.4.2. Finger-vein recognition

Nowadays, finger-vein recognition is also an emerging technique. As the light attenuation in biological tissue, it is easy to be degraded for the collected finger-vein images. That can lead to the finger-vein feature representation to be unreliable one. For this reason, it is required to enhance the finger-vein image for finger-vein based personal recognition. In [68], Yang et al. analyzed the intrinsic factors that can degrade of finger-vein images and proposed a method for the visibility improvement of finger-vein images.

And also, they proposed a directional filtering method relied on Gabor filters to handle venous region enhancement problem effectively. They also used a Phase-Only-Correlation strategy for the similarity measuring of the enhanced finger-vein images. In [69], Yang et al. presented a multimodal personal recognition system. They designed an image acquisition device to get the finger dorsal images and finger vein. And, they performed a unique registration on two kinds of images for utilizing the intrinsic positional relationship between the finger dorsal and the finger veins. At the feature level, they explored Comparative Competitive Code(C^2Code) and combine for finger vein and dorsal fusion. And at last, they input the C^2Code feature map into a Nearest Neighbor (NN) classifier for the achievement of personal authentication.

In [70], Wu et al. proposed a finger-vein pattern recognition algorithm that concerned with Support Vector Machine (SVM) and neural network technique. In the system, with the use of infrared Light-Emitting Diode (LED) and a Charged-coupled Device (CCD) camera, the pattern is taken to easily observe in visible light. It consists of pattern classification and image processing. For the pre-processing of the image, they also applied Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) as feature extraction and dimension reduction. In [71], for finger vein recognition, a novel Discriminative Binary Code (DBC) learning method was proposed. In this method, the obtained binary templates provide supervised information for the instances training, and SVMs are trained as the code learner for each bit. And also, for the discriminating of the codes, maximizing inter-class scatter and entropy is also proposed.

3.5. Spoof fingerprint detection

In accordance with the increasing of fingerprint recognition systems usage in both government and civilian applications, artificial fingerprint detection has been emergence as a new demanding research direction. Therefore, many researchers have also focused on the detection of the spoof fingerprints. Joshua et al. also presented a one class classifier for spoof detection to reduce the vulnerability of spoof detectors and expose attacks from spoofs that cannot be visible during the detector's training [72]. They used generative adversarial networks (GANs) to process live fingerprint images acquired by RaspiReader. It has been using Local Binary Pattern (LBP) as one of the best operators for the fingerprint detection method. However, it has some limitations in its spatial support area. For this reason, Jia et al. presented a novel spoof fingerprint detection method depending on the Multi-Scale Local Binary Pattern (MSLBP) [73]. The method can be implemented in two approaches for the spoof fingerprint detection. In both approaches, every MSLBP combined with a set of filters. And, each sample of LBP circle can collect intensity information from a large area. Furthermore, in [74], Tarang Chugh et al. proposed an approach based on deep convolutional neural network that utilizes local patches extracted throughout the fingerprint minutiae to develop accurate and generalizable algorithms for detecting fingerprint spoof attacks. In [75], Franco et al. also extensively discussed fingerprint-based biometric systems and potential issues of fingerprint scanners by creating artificial fingerprints. By using liveness detection, Reddy et al. proposed an anti-spoofing method based on pulse oximetry [76]. A method to collect data for spoof detection using a multispectral sensor has been discussed in [77].

4. Challenges and future research directions

According to our best knowledge, most of previous fingerprint classification research mostly based on k-means clustering, neural networks, SVM, Euclidian distance and nearest neighbor algorithms for the classification and training task and Gabor algorithm for the fingerprint image enhancement task. And they usually implement based on directional and positional of the print minutiae features (core and delta). And in accordance with the importance growing of the fingerprint usage in our daily lives, it is increasingly essential for the prevention of spoof fingerprints such as MasterPrints.

As fingerprints can reveal the daily routine of our lifestyle from mass spectrometry imaging of chemical compounds [78], fingerprint is one of the most essential evidence in the detecting the suspects because of its uniqueness and chemical information contained in the print. According to our knowledge, we can also research on fingerprint by combining with the chemical technology and machine learning technology, then the identity is inevitably discovered for the suspect accurately.

Concerned with fingerprint matching algorithms, it they can be considered based on general image correlation, skeleton matching, phase matching and minutiae matching. Among these four techniques, minutiae-based matching is widely applied. This is because it has already been successfully relied on minutiae many years ago by forensic examiners. And also, minutiae-based representation is the efficient of the storage and it is admissible the testimony for the suspect identity relying on minutiae in the law courts.

Currently, the minutiae matching research direction is to use local minutiae structures for discovering a coarse alignment between two fingerprints and concentrate the local matching results as the global level [2].

Generally, this type of algorithm consists of four steps.

- Firstly, it calculates the similarity of the pairwise between the two fingerprints minutiae by analyzing the descriptions of the minutiae.
- Additionally, the alignment of the two fingerprints will be carried out in accordance with the most identical minutiae pair.
- Furthermore, it consists of the establishment for the minutiae correspondence-minutiae which are very similar not only in the location but also in the direction to be similarity minutiae.
- At last, it calculates the closeness of the score for indicating the match rate between the two fingerprints depending on the considerations such as the matching minutiae number, the matching minutiae ratio in the overlapping region of the two fingerprints, and the uniformity of the ridge count between the matching minutiae.

As the usage of fingerprint recognition in commercial and government applications has increased, the emergence of condensed, economical sensors and impressive processors requirements are also coupled for completely automated, greatly precise, real-time systems. And also, fingerprint spoof detection and the detection

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

of artificial fingerprint research technology are also very popular. It is challenging to develop these next-generation systems and technologies for the research environments.

Apart from these, there is still the shortage of antemortem fingerprint records, particularly in the developing countries. Furthermore, the capability to restore quality postmortem impressions can reduce the performance of fingerprints for the identification of the dead [18].

5. Conclusions

This paper has discussed the essential and fundamental of fingerprint and its processing in the area of the criminal investigation, law enforcement and the effective of identifying the body in the fatalities. Furthermore, we have presented its state-of-the-art fingerprint algorithms in the fields of classification, matching, feature extraction, recognition and fingerprint spoof detection. Additionally, we had presented fingerprint applications in our daily lives and highlighted for future fingerprint research opportunities.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors would like to thank the anonymous reviewers for their comments and suggestions on improving the manuscript. The research was partially supported by the Key R & D Program of Hunan Province (Grant No. 2018GK2051), the Leading Talent Program of Science and Technology of Hunan Province (Grant No. 2017RS3025), the China Scholarship Council (Grant No. 201706310080), and the International Postdoctoral Exchange Fellowship Program of China Postdoctoral Council (Grant No. OCPC20180024).

References

[1] R. Saferstein, Criminalistics: An Introduction to Forensic Science, Pearson Higher Ed, 2015.

[2] A.K. Jain, J. Feng, K. Nandakumar, Fingerprint matching, Computer 43 (2) (2010) 36–44.

[3] X. Si, J. Feng, J. Zhou, Y. Luo, Detection and rectification of distorted fingerprints, IEEE Trans. Pattern Anal. Mach. Intell. 37 (3) (2015) 555–568.

[4] A.I. Awad, Machine learning techniques for fingerprint identification: A short review, in: International Conference on Advanced Machine Learning Technologies and Applications, Springer, 2012, pp. 524–531.

[5] R. Wang, C. Han, Y. Wu, T. Guo, Fingerprint classification based on depth neural network, 2014, arXiv preprint arXiv:1409.5188.

[6] R. Wang, C. Han, T. Guo, A novel fingerprint classification method based on deep learning, in: 2016 23rd International Conference on Pattern Recognition, ICPR, IEEE, 2016, pp. 931–936.

[7] M.S. Ala Balti, Fingerprint verification based on back propagation neural network and minimum distance between singularities, J. Electr. Eng. (2013) 91–98.

[8] Y. Yao, G.L. Marcialis, M. Pontil, P. Frasconi, F. Roli, A new machine learning approach to fingerprint classification, in: Congress of the Italian Association for Artificial Intelligence, Springer, 2001, pp. 57–63.

[9] P. Bontrager, A. Roy, J. Togelius, N. Memon, DeepMasterPrint: Fingerprint spoofing via latent variable evolution, 2017, arXiv preprint arXiv:1705.07386.

[10] A. Roy, N. Memon, A. Ross, Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems, IEEE Trans. Inf. Forensics Secur. 12 (9) (2017) 2013–2025.

[11] X. Si, J. Feng, J. Zhou, Y. Luo, Detection and rectification of distorted fingerprints, IEEE Trans. Pattern Anal. Mach. Intell. 37 (3) (2015) 555–568.

[12] S. Gu, J. Feng, J. Lu, J. Zhou, Efficient rectification of distorted fingerprints, IEEE Trans. Inf. Forensics Secur. 13 (1) (2018) 156–169.

[13] P.J. Kellman, J.L. Mnookin, G. Erlikhman, P. Garrigan, T. Ghose, E. Mettler, D. Charlton, I.E. Dror, Forensic comparison and matching of fingerprints: using quantitative image measures for estimating error rates through understanding and predicting difficulty, PLoS One 9 (5) (2014) e94617.

[14] P.M.-A. Hambalık, Fingerprint recognition system using artificial neural network as feature extractor: design and performance evaluation, Tatra Mt. Math. Publ. 67 (2016) 117–134.

[15] S. Sathyadevan, S. Gangadharan, et al., Crime analysis and prediction using data mining, in: 2014 First International Conference on Networks & Soft Computing, INSC2014, IEEE, 2014, pp. 406–412.

[16] S. Kouamo, C. Tangha, Fingerprint recognition with artificial neural networks: Application to e-learning, J. Intell. Lear. Syst. Appl. 8 (02) (2016) 39.

[17] L. O'Gorman, An overview of fingerprint verification technologies, Inf. Secur. Tech. Rep. 3 (1) (1998) 21–32.

[18] N. Kaushal, P. Kaushal, Human identification and fingerprints: A review, J. Biomet. Biostat. 2 (123) (2011) 2.

[19] P. Baldi, Y. Chauvin, Neural networks for fingerprint recognition, Neural Comput. 5 (3) (1993) 402–418.

[20] M. Kamijo, Classifying fingerprint images using neural network: Deriving the classification state, in: IEEE International Conference on Neural Networks, IEEE, 1993, pp. 1932–1937.

[21] S.M. Mohamed, H. Nyongesa, Automatic fingerprint classification system using fuzzy neural techniques, in: 2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No. 02CH37291), vol. 1, IEEE, 2002, pp. 358–362.

[22] Online Digital Education Connection, http://www.odec.ca/projects/2004/fren4j0/public_html/fingerprint_identification.htm, 2012.

[23] S. Wang, W.W. Zhang, Y.S. Wang, Fingerprint classification by directional fields, in: Proceedings. Fourth IEEE International Conference on Multimodal Interfaces, IEEE, 2002, pp. 395–399.

[24] X. Tan, B. Bhanu, Y. Lin, Learning features for fingerprint classification, in: International Conference on Audio-and Video-Based Biometric Person Authentication, Springer, 2003, pp. 318–326.

[25] P. Ramo, M. Tico, V. Onnia, J. Saarinen, Optimized singular point detection algorithm for fingerprint images, in: Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205), vol. 3, IEEE, 2001, pp. 242–245.

[26] C.H. Park, H. Park, Fingerprint classification using fast Fourier transform and nonlinear discriminant analysis, Pattern Recognit. 38 (4) (2005) 495–503.

[27] S. Shah, P.S. Sastry, Fingerprint classification using a feedback-based line detector, IEEE Trans. Syst. Man Cybern. B 34 (1) (2004) 85–94.

[28] L. Ji, Z. Yi, SVM-Based fingerprint classification using orientation field, in: Third International Conference on Natural Computation, ICNC 2007, vol. 2, IEEE, 2007, pp. 724–727.

[29] J. Li, W.-Y. Yau, H. Wang, Combining singular points and orientation image information for fingerprint classification, Pattern Recognit. 41 (1) (2008) 353–366.

[30] J. Zhou, J. Gu, D. Zhang, Singular points analysis in fingerprints based on topological structure and orientation field, in: International Conference on Biometrics, Springer, 2007, pp. 261–270.

[31] N. Nain, B. Bhadviya, B. Gautam, D. Kumar, B. Deepak, A fast fingerprint classification algorithm by tracing ridge-flow patterns, in: 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, IEEE, 2008, pp. 235–238.

[32] C. Museum, Foreinsic investigation, https://www.crimemuseum.org/crime-library/forensicinvestigation/fingerprints/.

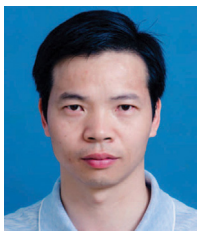
[33] L. Wei, Fingerprint classification using singularities detection, Int. J. Math. Comput. Simul. 2 (2) (2008) 158–162.

[34] M.H. Bhuyan, S. Saharia, D.K. Bhattacharyya, An effective method for fingerprint classification, 2012, arXiv preprint arXiv:1211.4658.

[35] M. Tarjoman, S. Zarei, Automatic fingerprint classification using graph theory, in: Proceedings of World Academy of Science, Engineering and Technology, vol. 30, 2008, pp. 831–835.

[36] F. Ahmad, D. Mohamad, A review on fingerprint classification techniques, in: 2009 International Conference on Computer Technology and Development, vol. 2, IEEE, 2009, pp. 411–415.
[37] J.W. Bond, The value of fingerprint evidence in detecting crime, Int. J. Police Sci. Manag. 11 (1) (2009) 77–84.
[38] V.C. Nayak, P. Rastogi, T. Kanchan, S.W. Lobo, K. Yoganarasimha, S. Nayak, N.G. Rao, G.P. Kumar, B.S.K. Shetty, R.G. Menezes, Sex differences from fingerprint ridge density in the Indian population, J. Forensic Leg. Med. 17 (2) (2010) 84–86.
[39] E. Gutiérrez-Redomero, C. Alonso, E. Romero, V. Galera, Variability of fingerprint ridge density in a sample of Spanish caucasians and its application to sex determination, Forensic Sci Int 180 (1) (2008) 17–22.
[40] M.A. Acree, Is there a gender difference in fingerprint ridge density? Forensic Sci Int 102 (1) (1999) 35–44.
[41] U.S. department of Homeland security, www.dhs.gov/usvisit, 2012.
[42] J.J. Engelsma, K. Cao, A.K. Jain, Raspireader: Open source fingerprint reader, IEEE Trans. Pattern Anal. Mach. Intell. (2018).
[43] K. Karu, A.K. Jain, Fingerprint classification, Pattern Recognit. 29 (3) (1996) 389–404.
[44] B. Fang, H. Wen, R.-Z. Liu, Y.-Y. Tang, A new fingerprint thinning algorithm, in: 2010 Chinese Conference on Pattern Recognition ,CCPR, IEEE, 2010, pp. 1–4.
[45] L. Ji, Z. Yi, L. Shang, X. Pu, Binary fingerprint image thinning using template-based pcnns, IEEE Trans. Syst. Man Cybern. B 37 (5) (2007) 1407–1413.
[46] V. Espinosa-Duro, Fingerprints thinning algorithm, IEEE Aerosp. Electron. Syst. Mag. 18 (9) (2003) 28–30.
[47] N.P. Khanyile, J.-R. Tapamo, E. Dube, A comparative study of fingerprint thinning algorithms, 2011.
[48] V. Espinosa-Duro, Fingerprints thinning algorithm, IEEE Aerosp. Electron. Syst. Mag. 18 (9) (2003) 28–30.
[49] S. Golabi, S. Saadat, M.S. Helfroush, A. Tashk, A novel thinning algorithm with fingerprint minutiae extraction capability, Int. J. Comput. Theory Eng. 4 (4) (2012) 514.
[50] B.-H. Cho, J.-S. Kim, J.-H. Bae, I.-G. Bae, K.-Y. Yoo, Fingerprint image classification by core analysis, in: WCC 2000-ICSP 2000. 2000 5th International Conference on Signal Processing Proceedings. 16th World Computer Congress 2000, vol. 3, IEEE, 2000, pp. 1534–1537.
[51] W. Liu, Y. Chen, F. Wan, Fingerprint classification by ridgeline and singular point analysis, in: 2008 Congress on Image and Signal Processing, vol. 4, IEEE, 2008, pp. 594–598.
[52] C. Kant, R. Nath, Reducing process-time for fingerprint identification system, Int. J. Biom. Bioinform. 3 (1) (2009) 1–9.
[53] D. Peralta, S. García, J.M. Benitez, F. Herrera, Minutiae-based fingerprint matching decomposition: methodology for big data frameworks, Inform. Sci. 408 (2017) 198–212.
[54] W. Lee, S. Cho, H. Choi, J. Kim, Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners, Expert Syst. Appl. 87 (2017) 183–198.
[55] X. Si, J. Feng, B. Yuan, J. Zhou, Dense registration of fingerprints, Pattern Recognit. 63 (2017) 87–101.
[56] D. Peralta, M. Galar, I. Triguero, D. Paternain, S. García, E. Barrenechea, J.M. Benítez, H. Bustince, F. Herrera, A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation, Inform. Sci. 315 (2015) 67–87.
[57] M. Galar, J. Derrac, D. Peralta, I. Triguero, D. Paternain, C. Lopez-Molina, S. García, J.M. Benítez, M. Pagola, E. Barrenechea, et al., A survey of fingerprint classification Part I: Taxonomies on feature extraction methods and learning models, Knowl.-Based Syst. 81 (2015) 76–97.
[58] D. Michelsanti, Y. Guichi, A.-D. Ene, R. Stef, K. Nasrollahi, T.B. Moeslund, Fast fingerprint classification with deep neural network, in: International Conference on Computer Vision Theory and Applications, SCITEPRESS Digital Library, 2018, pp. 202–209.
[59] S. Barra, M. De Marsico, M. Nappi, F. Narducci, D. Riccio, A hand-based biometric system in visible light for mobile environments, Inform. Sci. 479 (2019) 472–485.
[60] S. Ding, W. Bian, T. Sun, Y. Xue, Fingerprint enhancement rooted in the spectra diffusion by the aid of the 2D adaptive chebyshev band-pass filter with orientation-selective, Inform. Sci. 415 (2017) 233–246.
[61] M.A. Khan, T.M. Khan, D.G. Bailey, Y. Kong, A spatial domain scar removal strategy for fingerprint image enhancement, Pattern Recognit. 60 (2016) 258–274.
[62] M. Lastra, J. Carabaño, P.D. Gutiérrez, J.M. Benítez, F. Herrera, Fast fingerprint identification using GPUs, Inform. Sci. 301 (2015) 195–214.
[63] R. Cappelli, M. Ferrara, D. Maltoni, Large-scale fingerprint identification on GPU, Inform. Sci. 306 (2015) 1–20.
[64] D. Peralta, I. Triguero, S. García, F. Herrera, J.M. Benitez, DPD-DFF: A dual phase distributed scheme with double fingerprint fusion for fast and accurate identification in large databases, Inf. Fusion 32 (2016) 40–51.
[65] M.A. Medina-Pérez, A.M. Moreno, M.Á.F. Ballester, M. García-Borroto, O. Loyola-González, L. Altamirano-Robles, Latent fingerprint identification using deformable minutiae clustering, Neurocomputing 175 (2016) 851–865.
[66] D. Peralta, I. Triguero, S. García, Y. Saeys, J.M. Benitez, F. Herrera, Distributed incremental fingerprint identification with reduced database penetration rate using a hierarchical classification based on feature fusion and selection, Knowl.-Based Syst. 126 (2017) 91–103.
[67] J. Khodadoust, A.M. Khodadoust, Fingerprint indexing based on minutiae pairs and convex core point, Pattern Recognit. 67 (2017) 110–126.
[68] J. Yang, Y. Shi, Towards finger-vein image restoration and enhancement for finger-vein recognition, Inform. Sci. 268 (2014) 33–52.
[69] W. Yang, X. Huang, F. Zhou, Q. Liao, Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion, Inform. Sci. 268 (2014) 20–32.
[70] J.-D. Wu, C.-T. Liu, Finger-vein pattern identification using SVM and neural network technique, Expert Syst. Appl. 38 (11) (2011) 14284–14289.
[71] X. Xi, L. Yang, Y. Yin, Learning discriminative binary codes for finger vein recognition, Pattern Recognit. 66 (2017) 26–33.
[72] J.J. Engelsma, A.K. Jain, Generalizing fingerprint spoof detector: Learning a one-class classifier, 2019, arXiv preprint arXiv:1901.03918.
[73] X. Jia, X. Yang, K. Cao, Y. Zang, N. Zhang, R. Dai, X. Zhu, J. Tian, Multi-scale local binary pattern with filters for spoof fingerprint detection, Inform. Sci. 268 (2014) 91–102.
[74] T. Chugh, K. Cao, A.K. Jain, Fingerprint spoof detection using minutiae-based local patches, in: 2017 IEEE International Joint Conference on Biometrics, IJCB, IEEE, 2017, pp. 581–589.
[75] A. Franco, D. Maltoni, Fingerprint synthesis and spoof detection, in: Advances in Biometrics, Springer, 2008, pp. 385–406.
[76] P.V. Reddy, A. Kumar, S. Rahman, T.S. Mundra, A new method for fingerprint antispoofing using pulse oximetry, in: 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems, IEEE, 2007, pp. 1–6.
[77] K.A. Nixon, R.K. Rowe, Multispectral fingerprint imaging for spoof detection, in: Biometric Technology for Human Identification II, vol. 5779, International Society for Optics and Photonics, 2005, pp. 214–225.
[78] P. Hinners, K.C. O'Neill, Y.J. Lee, Revealing individual lifestyles through mass spectrometry imaging of chemical compounds in fingerprints, Sci. Rep. 8 (1) (2018) 5149.

Khin Nandar Win received B.Sc (Hons:) (Computer Science) from Yadanbon University in 2009 and M.Sc (Computer Science) from Yangon University in 2012 respectively. She is now currently a Ph.D. candidate in the College of Computer Science and Electronic Engineering, Hunan University. Her major research interests include spatio-temporal analysis, criminal analysis, fingerprint analysis, cloud computing, big data, pattern mining, and machine learning.



Kenli Li received the Ph.D. degree in computer science from Huazhong University of Science and Technology, China, in 2003. He was a visiting scholar at University of Illinois at Urbana-Champaign from 2004 to 2005. He is currently a full professor of computer science and technology at Hunan University and deputy director of National Supercomputing Center in Changsha. His major research includes *parallel computing, cloud computing, and Big Data computing*. He has published more than 150 papers in international conferences and journals, such as *IEEE-TC, IEEE-TPDS, IEEE-TSP*. He is currently serving on the editorial boards of IEEE Trans. on Computers, International Journal of Pattern Recognition and Artificial Intelligence. He is a senior member of IEEE and an outstanding member of CCF.

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.

Jianguo Chen received the Ph.D. degree from the College of Computer Science and Electronic Engineering, Hunan University, China. He was a visiting Ph.D. student at the University of Illinois at Chicago from 2017 to 2018. He is currently a postdoctoral with the University of Toronto and Hunan University. His major research interests include parallel computing, cloud computing, machine learning, data mining, bioinformatics and big data.

Philippe Fournier-Viger received the Ph.D. degree in computer science from the University of Quebec, Montreal, in 2010. He is currently a Professor with the Shenzhen Graduate School, Harbin Institute of Technology, China. He is also the Founder of the popular SPMF open-source data mining library, which has been cited in over 430 research papers since 2010. He has published over 140 research papers in refereed international conferences and journals, which have received over 1,300 citations. His research interests include data mining, pattern mining, sequence analysis and prediction, text mining, e-learning, and social network mining. He has received the title of Youth 1000 Talent from the National Science Foundation of China. He is the Editor-in-Chief of the Data Mining and Pattern Recognition Journal.

Keqin Li is a SUNY Distinguished Professor of computer science in the State University of New York. He is also a Distinguished Professor of Chinese National Recruitment Program of Global Experts (1000 Plan) at Hunan University, China. He was an Intellectual Ventures endowed visiting chair professor at the National Laboratory for Information Science and Technology, Tsinghua University, Beijing, China, during 2011–2014. His current research interests include parallel computing and high-performance computing, distributed computing, energy-efficient computing and communication, heterogeneous computing systems, cloud computing, big data computing, CPU–GPU hybrid and cooperative computing, multicore computing, storage and le systems, wireless communication networks, sensor networks, peer-to-peer le sharing systems, mobile computing, service computing, Internet of things and cyber–physical systems. He has published over 520 journal articles, book chapters, and refereed conference papers, and has received several best paper awards. He is currently or has served on the editorial boards of IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Computers, IEEE Transactions on Cloud Computing, IEEE Transactions on Services Computing, and IEEE Transactions on Sustainable Computing. He is an IEEE Fellow.

Please cite this article as: K.N. Win, K. Li, J. Chen et al., Fingerprint classification and identification algorithms for criminal investigation: A survey, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.10.019.