A Review on Fingerprint Recognition Techniques

Suraj S. Khairnar[1], Prof. Sameena Zafar[2]
[1]M.Tech Student, [2]Associate Professor
[1, 2]Patel college of Science and Technology, Raitbad, Bhopal, India

Abstract - With increasing demand for applications in biometric security and privacy, the field of fingerprint recognition attracts many researchers. Accomplishment of reduced verification error rate while higher security and privacy is needful in the present demanding environment. Many applications are demanding for less probability to reveal person's identity, faster and good verification results for fingerprint. In this paper, authors have reviewed abundant attempts made by researchers to fulfill the requirement of fingerprint authentication and security. One of the best choices for fingerprint recognition was devices which having specific quality to capture images which are fused together that replaced by decomposition algorithm. Authors have presented state of art for various methods in fingerprint recognition area. With the advancement in research in the fields namely mixing fingerprint to latent person's identity and algorithm in all aspects.

Keywords: Minutiae, feature extraction, continuous and spiral component.

I. INTRODUCTION

Impression made by the minute ridge formation or patterns found on fingertips is identification mark of person in fingerprint recognition. In fingerprinting a person's fingertip is stored as image and image is recorded by its characteristics as loops , arches and whorls along the pattern of minutiae ,furrows and ridges. A digital image of the fingerprint pattern is captured by using a fingerprint sensor. To store a collection of extracted features i.e a biometric template which is stored and used for matching[1]. For authentication purposes using matching algorithm stored templates of fingerprints compared against candidate fingerprints

This is done either by directly comparing the original image with the candidate image or by comparing certain features. Direct (optical) correlation uses general shape of the fingerprint to preprocess the images and search in large databases are reduced, which is in efficient due to large database hence practically not used. Most of the algorithms uses minutiae, the particular points such as bifurcation, ridges ending. For further comparison direction and position of these features are stored in the identification in authentication. While some algorithm computes the minutiae instead of the distances from the position number of ridges between specific points are counted Pattern matching algorithms uses usual shape of the ridges. In which fingerprint is sectioned into ridge direction and small sectors, pitch and phase are extracted and stored. General directions of the lines of the fingerprint and the presence of the core and the delta are used. Most algorithms are using minutiae, the particular points like bifurcation, ridges ending. Only the direction and position of these features are stored in the signature for further comparison [1].

Mixing fingerprints used for authentication by creating a new virtual identity. The original identities of subjects can be concealing by using these virtual identities. The mixed image contains characteristics from both the original fingerprint images, this image can used directly in feature extraction and matching stages of an existing fingerprint recognition system [2].

To create a new identity two fingerprints acquired from two different fingers are fused together. A new identity image i.e. mixed image holds the characteristics of both the actual images, which can be used without an intermediary in feature extraction and matching steps of an existing system. At first, each fingerprint is decomposed into two different components viz. continuous and spiral components. The continuous portion gives details of the domestic ridge orientation, and the spiral portion describes the minutiae position. Next, the two elements of each fingerprint are aligned to a common coordinate system. Finally, the continuous element of one fingerprint is combined with the spiral element of the other fingerprint [3].

This work explores the possibility of mixing two separate fingerprints at the image point in order to generate a new fingerprint identity.

II. PATTERNS OF FINGERPRINT

For matching fingerprints analysis is finished by correlation of varied options of the print models. These contain models, that area unit combination characteristics of ridges, and item points, that area unit distinctive options found among the patterns [4]. The three basic patterns of fingerprint ridges area unit the arch, loop, and whorl:

Arch: Arches area unit found in concerning five-hitter of fingerprint patterns encountered. The ridges run from one facet to the opposite of the pattern, creating no backward flip. Ordinarily, there's no delta in Associate in Nursing arch pattern however wherever there a delta, no re-curving ridge should intervene between the core and delta points

Loops: occur in concerning 60-70 you rather than fingerprint patterns encountered. One or additional of the ridges enters on either facet of the impression, re-curves, touches or crosses the road going from the delta to the core and stop on or within the direction of the facet wherever the ridge or ridges entered.

Whorls: area unit seen in concerning 25-35 you rather than fingerprint patterns encountered. In a whorl, a number of the ridges build a flip through a minimum of one circuit. Any fingerprint pattern that contains a combine of or extra deltas area unit a whorl pattern.

Two illustration structure for fingerprints distinguishes the two approximations for fingerprint recognition. The primary approach, that is minutia-based, represents the fingerprint by its native options, like terminations and bifurcations. The second approach, that uses image-based ways, tries to try to matching supported the worldwide options of a full fingerprint image.

III. STORAGE AND SECURITY FOR FINGERPRINT RECOGNITION

In order to generate a new image , image level fusion refers to the combination of (a) different sensors are used to obtain multiple samples of the same biometric attribute or (b) single sensor is used to obtain multiple instances of same biometric attribute. In the context of fingerprints, image-level fusion has been used to combine multiple impressions of the same finger as exemplified in the following scenarios:

Multispectral sensor

In [5], fused multiple images acquired from a multispectral fingerprint scanner into a single high quality fingerprint image.

Multiple images are captured by MSI sensor, which are subject to different illumination conditions, including different wavelengths, different polarization conditions and different illumination orientations.

The resulting statistics gives information about both the surface and subsurface features of the skin. A single composite fingerprint image is produced by processing this data which is same as that obtained by conventional fingerprint reader, but which has better performance characteristics

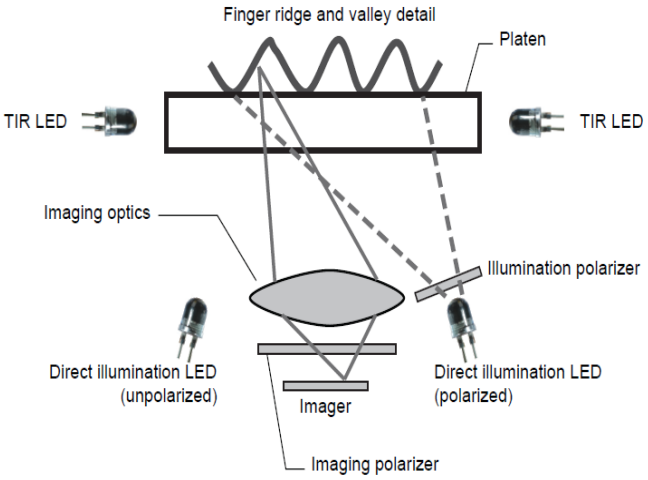

Fig.1. Optical Configuration of MSI Sensor [5]

MSI imaging sensor comes with the advantage to collect usable biometric images under conditions where other conventional sensor found deficient, such as moisture and bright ambient lights are present or when topical contaminants or there is poor contact between sensor and the finger.MSI details can be further processed to make sure that the measured optical characteristics equivalent those of living human skin, subjected to protect against attempts to spoof the sensor.

Small area sensor

There exist also some sensors those capture only a small portion of the fingertip [2]. One merit of small area sensor due to small size they can be used in many applications. Due to small physical size of small sensing area of small sensor, only limited information is stored about fingerprint, also due to small number of minutia, template features that are located, can restrict reliable authentication and due to small sensing area between the template impression and the query impression gives poor recognition performance. For example, a higher rate of false rejects. To overcome this several fingerprint mosaicing techniques [6], [7], [8] and [9]

1.One of the possible solutions to tackle such difficulties is to generate a composite fingerprint template during the enrollment phase when more than one fingerprint images of the same finger are often taken. [8],

2. The fingerprint fusion algorithm can be categorized largely into two types. The first type fuses feature sets from several fingerprint images; the second type produces a mosaicked fingerprint image with several images [7].

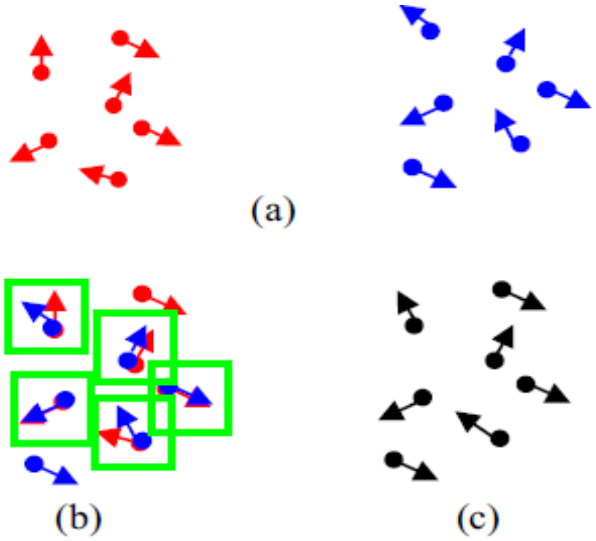

Fig.2. Template synthesis process (a) Two sets of minutiae template. (b) The minutiae template after using the bounding box for pairing (c) The resultant composite template[8]

3. Information content of the resulting fingerprint template can be combined to intensify the information from several impressions of a finger, process is known as mosaicing, which is supposed to enhance the matching performance of a fingerprint system. Mosaicking can be accomplished at two distinct levels: (a) the image level (image mosaicking), where multiple impressions of a finger are combined together to generate an elaborate fingerprint - minutiae points are then extracted from the mosaicked fingerprint; and (b) the feature level (feature mosaicking), where the minutiae sets extracted from multiple impressions are combined to generate a composite feature set. Fig.3 shows each schemes, each these schemes have confidence a strong registration technique to accurately align a try of impressions (or trivialities sets) before integration them. [9],

Multi-view sensor

To overcome the problem of touch-based sensing techniques, touch less fingerprint sensing technologies explored as any contact between a sensor and a finger is not essential. Touch less fingerprint sensors capture multiple views of a finger using several calibrated cameras.

The Surround Imager ,an innovative multi-camera touch less device able to capture rolled-equivalent fingerprints, the acquired image have no deformation, due to absence of contact between any rigid surface and the elastic skin of the finger.

The multi-view camera system provides 3D representations of fingerprint, different finger views are obtaining that are combined to form single 3-D image [10] or a single camera with two planar mirrors.

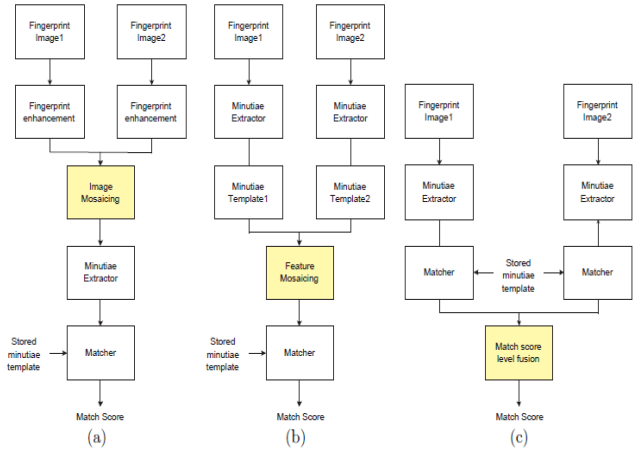

Fig.3.Information fusion in fingerprints: (a) Image mosaicing; (b) Feature mosaicing; (c) Match score level fusion[9].

In [11], three different views at a time is captured by a new touch less fingerprint sensing device, these view-different images are for mosaicing method. The device is combination of two planar mirrors which reflects side views of finger and one camera to capture images, this camera is best alternative to multiple camera based system as they are quite expensive.

In mosaic method can synthesize the multiple view images by expanding the functional area of fingerprint image with use of the thin plate spline model.

In final mosaicked image, a region in each view is selected such way that the ridge intervals are minimized so it will reduce the effect of perspective distortion. System is more reliable as experiments shown 28% larger good quality area than one-view, unavailable mosaicked images and 29% more minutiae, also it gives more matched minutiae than matching with frontal images when side view images are a=matched to mosaicked images.[11]

This method can be also beneficial for applications where large template is required for recognition. But these methods come along with some demerits of less functional area of touch less fingerprint image and some view difference problem.

IV. PRIVACY OF FINGERPRINT RECOGNITION

De-identifying a fingerprint image is necessary to mitigate concerns related to data misuse and data sharing [12]–[14].

To secure important data/images conventional cryptographic systems provide numerous ways. For encrypting templates of fingerprints there are two main concerns.

First, the stored template has to be decrypted during every identification/verification attempt (fingerprint cryptosystems are exception as matching can be done in the encrypted domain—but this affects matching performance). Second, the security of these algorithms depends on the considering that the only one of the main legitimate user is familiar with the cryptographic keys. Hence the one of main challenge in practical cryptosystem is to maintain secrecy of keys. Thus

Thus, the original fingerprint template will be exposed to eavesdroppers. The stolen templates could be used to reconstruct the original fingerprint image [15]–[18]; in other words, compromising a fingerprint template can result in permanent loss of a subject's biometric. Fingerprint mixing can be used to de-identify an input fingerprint image by fusing it with another fingerprint (e.g., a synthetic fingerprint) at image level, in order to obtain a new mixed image that complicates the identity of the original fingerprint.

Biometric data is replacing a password-based security system which shows its increased use in authentication and identification of individuals. Identification and authentication are two different tasks in relation to fingerprint recognition. Identification refers to finding the identity of a person given the biometric and authentication is termed as verification of the identity given the biometric data and the claimed identity

In [19], to address these privacy concerns a biometric framework is discussed. In particular, to obtain a non-unique identifier of single two biometric features (e.g. fingerprints) are integrated and stored as such in a main database. For privacy concerns, combined biometric ID is not only one identifier, but still it is shown that it can be used in authenticating a person's identity. An experimental demonstration has shown a fingerprint verification system to form a combined biometric ID, uses two separate fingerprints of same person. The discussed method creates two separate biometric IDs, one person can use two fingerprints for one application and other two fingerprints for another one (e.g., bank). Until and unless it is impossible to link these two databases, the person can be authenticated for any application.

Also, to search for a person it would be quite difficult to use hidden fingerprints in this system, as one would require attempting many such combinations of fingerprint pairs.

From the experimental evaluation with a system using fingerprints and it is proven by results that for minutiae detection and matching [19], even with very simple algorithms very small (2.1% EER) authentication error rate is obtained

In comparison with our simple fingerprint verification system,

The combined biometric system results into reduced verification error. Hence this without hiding verification process, this method can be used to increase privacy. This algorithm is proven that certain pattern of minutiae distribution appears the largest extent may possible. Also this algorithm is not claiming that mixed biometric cannot be used to reveal person's identity. In the future, one need to check for the algorithm for mixing fingerprints which disperse the minutiae points as much as possible such that most unique features of fingerprints will remain hidden.

V. MIXING FINGERPRINTS

In [3] a new method is proposed, which creates a new entity that replicates the plausible fingerprint image and thus, a) it is difficult to decide an intruder whether a print is mixed or not b) also conventional algorithm can be used to process it.

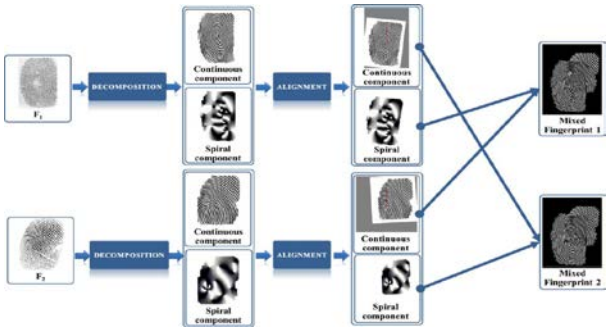

Fig.4. Mixing fingerprint approach in [3]

Hence the fingerprint mixing can be utilized to enhance the privacy of fingerprint recognition system.

Consider a distant fingerprint system shown in fig.4 that Maintains a little set of preselected auxiliary fingerprints, *A*, resembling multiple fingers (each finger during *A* is assumed to possess multiple impressions). Suppose that subject ID_s offers the left index fingerprint, FL_s , throughout enrollment at an area machine. At that point, the native machine decomposes the fingerprint FL_s , into two elements, i.e., the spiral part and also the continuous part. to make sure the privacy of the fingerprint image within the native system, the remote system transmits the fingerprints within the auxiliary set and also the native machine searches through the received Fingerprints to find a "compatible" fingerprint primarily based On the continual part of FL_s say $F_m \in A$ (here the subscript *m* denotes a particular finger within the auxiliary set), that is then rotten and its continuous part mixed with the spiral part of FL_s at the native Machine (see step (2) in Fig.4). The template of the new mixed print M_s is registered within the remote system info and FL_s is discarded from the native machine (see step (3) in Fig. 4). throughout authentication, once the topic presents a sample of the left finger,FL_s', it's rotten and its continuous part is employed to look through the fingerprints within the auxiliary set from the remote fingerprint system to see the foremost "compatible" fingerprint, say $F_n \in A$. within the native machine, the spiral part of $FL_s'$is mixed with the continual part of $F_n \in A$ to get a mixed fingerprint , that is then compared against the info entry M_s'. the protection protocol (illustrated in Fig. 4) ensures that in the enrollment or the authentication method, the identities of the users won't be discovered by the fingerprint system. Further, though the privacy of the input fingerprints is that the main concern, the privacy of the hold on auxiliary set, e.g., *A*, may well be preserved by storing simply the continual elements of the preselected fingerprints.

Different sized databases of virtual identities from fastened fingerprint dataset square measure generated by victimization the planned methodology (c) the blending method will be wont to obscure the knowledge gift in associate degree individual's fingerprint Image before storing it during a central database; and (d) the mixed fingerprint will be wont to generate a cancelable template, i.e., the template will be reset if the mixed fingerprint is compromised. As this paper offers elaborated study of security aspects i.e. non-invertibility and quality properties of the approach additionally this planned approach will be used for de-identifying fingerprints. This security analysis relies on metrics ordinarily employed in the cancelable life science literature.

Further work is needed to boost the performance thanks to mixed fingerprints by exploring alternate algorithms for prealigning, choosing and combination the various pairs.

VI. DISCUSSION AND CONCLUSIONS

In several applications, identification is enjoying important role in each facet. This review presents that advances in Fingerprint recognition is growing quicker. Still in progress analysis has been created this as a middle of attraction. Authors tried to work out a comprehensive and up to date progress during this review.

While handling standard fingerprint recognition system one cannot assure the protection of Person's personal details and once one going for combination fingerprint by image fusing approach they have to ensure for fewer verification error and high level authentication . The analysis accomplishment with the advancement on utilize combination fingerprint knowledge by moldering it and adding with dummy fingerprint knowledge , offers the upper level security and privacy for person's ID.

With the advancement as algorithmic rule that warranty non-invertibility and quality of saved fingerprint info. Still there\'s want for future algorithmic rule to provide correct pre orienting and provides the higher result or build a lot of biometric id for single person dataset by combination with completely different fingerprint dataset.

REFERENCES

[1] A. Ross, K. Nandakumar, and A. Jain,*Handbook of Multibiometrics*. New York: Springer-Verlag, 2006, New York Inc.

[2] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer-Verlag, 2009, New York Inc..

[3] Asem Othaman and Arun Ross ,On Mixing Fingerprints. *IEEE Trans.on information forensics and security.*, vol. 8, no. 1, Jan. 2013

[4] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security and Privacy*, 1998, pp. 148–157.

[5] R. Rowe, K. Nixon, and P. Butler. Multispectral fingerprint image acquisition. *Advances in Biometrics*, pages 3–23, 2008.

[6] N. Ratha, J. Connell, and R. Bolle. Image mosaicing for rolled fingerprint construction. In *ICPR*, volume 2, 1998.

[7] A. Jain and A. Ross. Fingerprint mosaicking. In *ICASSP*, volume 4, pages IV–4064 –IV–4067, 2002.

[8] Y. Moon, H. Yeung, K. Chan, and S. Chan. Template synthesis and image mosaicking for fingerprint registration: an experimental study. In *ICASSP*, volume 5, 2004.

[9] A. Ross, S. Shah, and J. Shah. Image versus feature mosaicing: a case study in fingerprints. In *SPIE BTHI*, pages 620208–1 – 620208–12, 2006.

[10] G. Parziale, E. Diaz-Santana, and R. Hauke. The surround imager tm: A multi-camera touchless device to acquire 3D rolled-equivalent fingerprints. In *Advances in Biometrics*, volume 3832, pages 244–250. Springer, 2005.

[11] H. Choi, K. Choi, and J. Kim. Mosaicing touchless and mirror-reflected fingerprint images. *TIFS*, 5(1):52–61, March 2010.

[12] A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in *Proc. Eur. Signal Processing Conf. (EUSIPCO)*, 2005, pp. 469–472.

[13] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security and Privacy*, 1998, pp. 148–157.

[14] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[15] A. Ross, J. Shah, and A. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007

[16] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[17] J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 2, pp. 209–223, Feb. 2011.

[18] S. Li and A. Kot, "Attack using reconstructed fingerprint," in *Proc.IEEE Int. Workshop Information Forensics and Security (WIFS)*, 2011, pp. 1–6.

[19] K. G. Larkin, D. J. Bone, and M. A. Oldfield. Natural demodulation of two-dimensional fringe patterns. I. General background of the spiral phase quadrature transform. *J. Opt. Soc. Am. A*, 18(8):1862–1870, 2001.