Received: April 16, 2023. Revised: August 29, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# An Effective Finger-Print Validation and Identification Using A-KAZE and SURF Algorithm

**Poornima E. Gundgurti[1]*** **Shrinivasrao B. Kulkarni[2]**

*[1]Department of Computer Science, VTU Centre for PG studies Kalaburagi*
*and Affiliated to Visvesvaraya Technological University, Belagavi-590018, Karnataka, India*
*[2]Department of Computer Science and Engineering, SDM College of Engineering and Technology, Dharwad,*
*and Affiliated to Visvesvaraya Technological University, Belagavi-590018, Karnataka, India*
* Corresponding author's Email: Poornimae25@gmail.com

**Abstract:** The identification of users through their fingerprints has been widely used in various applications such as biometrics, border control identification, payment gateways and so on. But a proper fingerprint validation system remains a major issue in precise detection and takes more time to process the fingerprints. To overcome these fore mentioned issues, this manuscript introduced an effective fingerprint validation system using the data collected from FVC 2000 DB1, FVC 2002 DB1 and FVC 2004 datasets. The pre-processing is supported for image enhancement using CLAHE algorithm equalization and normalization. Additionally, the signal images are effectively extracted by applying the A-KAZE and SURF extracted algorithm which helps to reduce the time required for feature extraction and description of the identification process. At the final stage, random sample consensus (RANSAC) algorithm is applied to identify and validate the fingerprint effectively with better accuracy. The elapse time of the proposed approach is 3.09 s whereas the elapse time of the automatic fingerprint-based authentication framework is 4.03 s and minutiae triangulation technique is 3.55 s. Similarly, when the proposed approach is evaluated with FVC 2004 dataset, the elapse time is 5.20 ms whereas the existing scale-invariant feature transform (SIFT) detector obtained elapse time of 4.35 s.

**Keywords:** Minutiae fingerprint identification, CLAHE, Histogram equalization, Ridge thinning, RANSAC feature selection.

## 1. Introduction

Today, everyone uses a mobile phone to manage their bank accounts, credit scores, trades, online shopping, etc. A highly secure identification solution, like biometrics, is needed to access the internet safely [1-2]. Every human has unique biometrics that can alter owing to certain unforeseen conditions. Biometrics describes an individual's physical traits, such as their fingerprint, palm print, face, ear, toe, hand geometry, and iris, as well as their behavioral traits, such as their movement, speech, voice, and signature, and chemical traits, such as their odor [3]. In most biometric systems, fingerprints play a crucial role in detecting personal identities, with uses ranging from identity recognition in forensic investigations to unlocking consumer smartphones [4-5]. Among biometric-based security solutions, fingerprints are the most widely used and appealing since their ability and uniqueness remain constant over a person's lifetime [6-8].

Additionally, fingerprints play a vital role in the biometric system which evaluates the ridge friction pattern of the fingers [9]. Because of this, the biometric characteristic is frequently used in a variety of applications including criminology, banking, health care, etc [10-11]. Where the latent fingerprints and impressions are compared between two different types of fingerprints. high-quality fingerprint impressions are obtained under carefully regulated circumstances due to numerous difficulties, including intra-class variability, inter-class similarity, segmentation, noisy input, scalability, and template size, designing biometric systems is a very challenging process [12]. To overcome the current challenges in recognizing the fingerprint of a person with imperfect and overlapping fingerprints, the proposed method introduced an enhanced recognition system that details the fingerprint of the individual in an effective way [13, 14]. This suggested technique addresses the current difficulties in identifying a person from fingerprint scans that are overlapping and of poor quality [15]. As a result, the focus of this research is on the feature identification and detection of the pertinent elements in tiny fingerprint image identification.

The main contribution of the research is given as follows:

1. In the existing approach, the count of inlier features leads to a rise in matching features whereas, the KAZE -SURF exhibits less variation in the matching score across all incidence angles, which contributes to its effectiveness as an image-to-detection technique.
2. Further RANSAC feature selection method can identify and discard points that are outliers to precisely pinpoint the matching area. Additionally, the performance of the proposed method is evaluated for images with higher invariance and transforming the image based on each feature of the images.

This research paper is presented as follows: the existing work related to minutiae fingerprint identification and detection are represented in section 2. The clear explanation of the A-KAZE- SURF algorithm is explained in section 3. Minutiae fingerprint extraction and matching are analysed in sections 4 and 5. The result and discussion are presented in section 6. The conclusion of this research work is presented in section 7.

## 2. Literature survey

This section provides a literature survey about the different techniques used in fingerprint identification and verification. The following presents the literature survey along with the advantages and limitations.

Octavio Loyola-González [16] created the improved datasets to train the multiple ML models to forecast how missing details will affect a fingerprint recognition system's matching score. In this study, they employed two alternative matching algorithms, such as minutia cylinder-code (MCC) and deformable minutiae clustering using cylinder-codes (DMCCC), together with the typical NIST SD27 datasets to eliminate ground truth minutia from the latent fingerprint. Therefore, removing the fine details of the positive and negative impacts would improve the prediction of the matching score, but it has a large false positive value that suggested blind verification of the system.

Samy Bakheet [17] represented the Harris and SURF feature detection method using the FVC2000 DBI datasets to perform an automatic fingerprint-based authentication framework which improved each person's identity system. First, a CLAHE form of adaptive histogram equalization using FFT and Gabor riddles was used to increase the difference of the input impression images. After that, two separate combination detection algorithms were used to extract the feature images and apply authentication. As a result, the authentication framework has an average recognition rate and system viability, but it also has a high level of robustness and mistake rate.

Yumnam Surajkanta [18] introduced a digital geometry fingerprint template based on FVC2000 fingerprint datasets and the translation and rotation invariant properties of the Delaunay triangulation of minutiae matching algorithms. Additionally, to boost discriminative strength and prevent false matches with local ridges and the core information, the gathered aspects were added to the templates and recorded, including the minutiae type and angles of the triangles. Therefore, the fingerprint templates were an effective enhancement over the traditional method and perform well in the identification procedure. The minutiae pattern only captured the uniqueness of a fingerprint and it is negatively impacted by noise and errors during extraction which leads to the absence or presence of minutiae in the pattern.

Sidra Aleem [19] represented an automated cyber-physical system with enhanced security biometric identification capabilities that uses the system's face and fingerprint to effectively authenticate personal identity. Additionally, the system merged its two core modules—enrolment and system identification. The obtained fingerprint was subjected to pre-processing and matching using an elastic technique that is alignment-based. As a result, the cyber-physical system was able to achieve higher identification accuracy and effective features in more realistic parts-based representations, even though the performance can be greatly impacted by lighting, distance to the surveillance camera, equipment, and operator training.

Amit Kumar Trivedi [20] demonstrate a unique minutiae triangulation technique that was developed for Non-Invertible Fingerprint Template Generation utilizing FVC2000 datasets. The minutiae of a

Received: April 16, 2023. Revised: August 29, 2023.

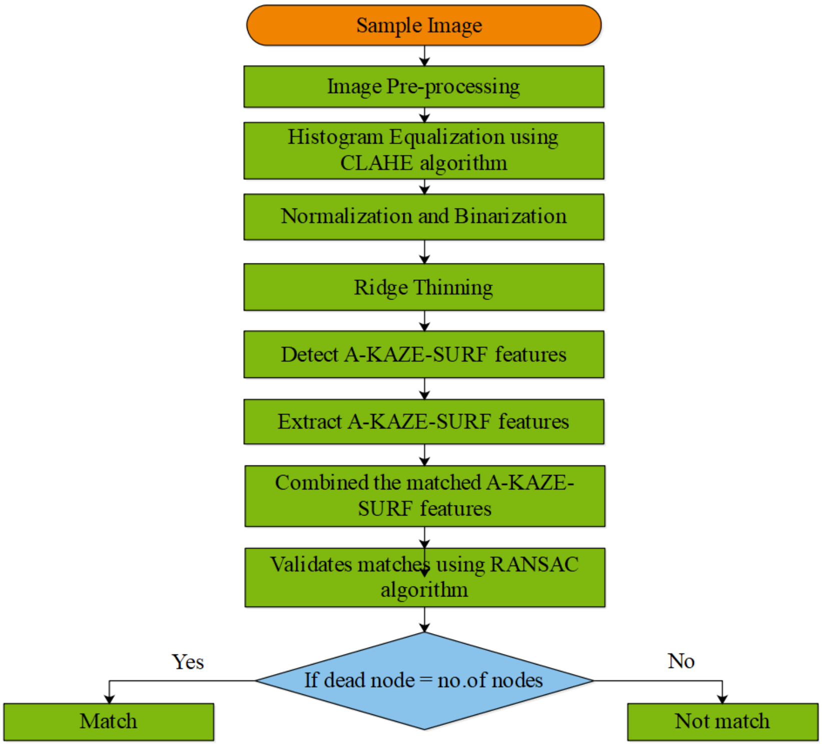
Sample Image
Image Pre-processing
Histogram Equalization using CLAHE algorithm
Normalization and Binarization
Ridge Thinning
Detect A-KAZE-SURF features
Extract A-KAZE-SURF features
Combined the matched A-KAZE-SURF features
Validates matches using RANSAC algorithm
If dead node = no.of nodes
Yes
No
Match
Not match

Figure. 1 The proposed A-KAZE –SURF minutiae feature extraction

template were used in this triangulation process to create a series of minutiae triplets, each of which forms a strong fingerprint template. Additionally, the function's adaptive threshold was used to analyse the triplet set. Therefore, the minutiae triangulation technique was effective in terms of the system's equal error rate, but it would require less security for the transmission of the template database.

Eain Ul Sehar [21] have introduced a cancellable approach for protection of fingerprint templates (FinCaT) using quadrant mapping through non-invertible transformation function. The FinCaT approach converts the original fingerprint templates to a secured template which maps minutia points using distinct parameters at each quadrant. Th suggested approach offers high revocability with newly created templates. However, the suggested approach does not consider the dimensional location of the minutiae which may results in false recognition for minute finger prints.

Samy Bakheet [22] have introduced an automated minutiae extraction and matching framework using a scale-invariant feature transform (SIFT) detector to enhance the quality of latent fingerprints. Moreover, brute force algorithm was used to store the templates by evaluating the Euclidean distance among SIFT and matched key points. At last stage, dual threshold filter was used to eliminate the false matched finger prints. However, the suggested approach using SIFT was validated with minimal number of latent finger prints.

## 3. A-KAZE-SURF methodology

In this research, the enhanced individual fingerprint identification was performed based on enhanced KAZE and SURF algorithms and feature outliers by using the random sample consensus (RANSAC) algorithm. The performance of fingerprint identification consists of datasets, Preprocessing, feature extraction, removing outliers' function, and matching. The block diagram of the proposed research is shown in Fig. 1.

### 3.1 Data acquisition

This research utilized two publicly accessible datasets such as FVC2000 DB1 [23], FVC2002 DB1[24] and FVC 2004 [25] database to collect the fingerprint samples. All testing and assessment studies employ FVC2000 DB1 and FVC2002 DB1 datasets, which are comprised of 80 impression images with a determination of 300 ×300 pixels for FVC2000 DB1 and 388× 374 pixels for FVC2002 DB. Both datasets are freely downloadable by the general public and include 10 separate people's fingerprint images, eight of which were captured with the same finger. The data present in FVC 2004 dataset are gathered with the aim of creating difficult benchmark because the top methodologies attained

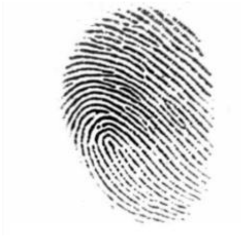

Figure. 2 Original input image of FVC 2000 DB1

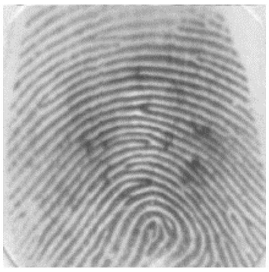

Figure. 3 Original input image of FVC 2002 DB1

accuracies close to 100 percent. The FVC 2004 data was acquired from students with each set containing 880 fingerprints from 110 fingers. The original image of the minutiae fingerprint identification of the FVC 2000 DB and FVC 2002 DB datasets is shown in Fig. 2 and Fig. 3.

### 3.2 Fingerprint image pre-processing:

The pre-processing is essential to get rid of all these artifacts and aid in the function's ability to effectively detect fingerprints. The information from the system's sensors and/or other media was used to determine the quality of the fingerprint images. Consequently, the presence of noise caused the image to lose the sharpness of the ridge structure. Additionally, the identification process is negatively impacted by the mode of image acquisition and the discontinuities between different feature vectors. Therefore, before the identification process, all of these artifacts must be eliminated.

#### 3.2.1. Histogram equalization

After eliminating the unwanted noise, the histogram equalization process was utilized to allocate the grey level in the input images and also enhance the vividness of the pixel based on images. The cumulative distribution function of the pixel values in an image is used in the representative image-enhancing technique known as histogram equalization. This process uses an advanced histogram equalization technique called contrast limited adaptive histogram equalization to effectively reset the illumination charge of every pixel based on the twin histogram as well as the intent and spread the pixel value circulation for improving the perceptional evidence (CLAHE). Locally, the CLAHE function increased contrast and integrated neighboring tiles using a bilinear interpolation function on the input image's tiny sections known as tiles. It was repeated until there were more than 1000 pixels in the ranges 0-49 and 206-255 in the histogram, after which the system's false bounds were erased. As a result, the average intensity and contrast of the fingerprint photos will be improved in this histogram image. The histogram equalization of the minute fingerprint identification of the FVC 2000 DB and FVC 2002 DB datasets is shown in Fig. 4 and Fig. 5.

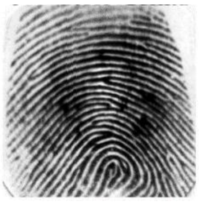

Figure. 4 Histogram equalized image-FVC2000-DB

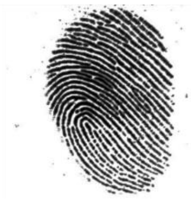

Figure. 5 Histogram equalized image-FVC-2002 DB

#### 3.2.2. Normalization

Normalization, commonly referred to as contrast stretching, is the process of modifying the range of pixel intensity values. This method is a short and crucial pre-dispensation step that can increase the eminence of the image by removing the noise. An image is normalized by adjusting the brightness of each pixel, which reduces the image as a whole to a set of predetermined values. Normalization is a function that upholds the sharpness and difference of the edges and valleys construction on a pixel-by-pixel basis. The normalized image of $N(i,j)$ is defined in Eq. (1):

$$N(i,j) = \begin{cases} \frac{M_0+\sqrt{VAR_0(I(i,j)-M)^2}}{VAR}, & if\ I(i,j) > M \\ \frac{M_0-\sqrt{VAR_0(I(i,j)-M)^2}}{VAR}\ , & otherwise \end{cases} \quad (1)$$

Where $M_0$ and $VAR_0$ denotes values of mean and variance which are represented in Eq. (2)

$$M(1) = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j),\ \ VAR\ (I) = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} (I(i,j) - M(I))^2 \quad (2)$$

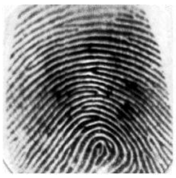

Figure. 6 Normalized image of FVC 2000 DB

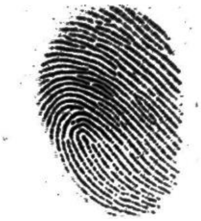

Figure. 7 Normalized image of FVC 2002 DB

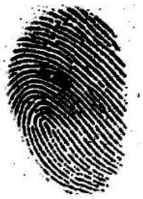

Figure. 8 After Binarized of the minutiae fingerprint image

The variance values in this equation are set to $M_0 = 0$ and $VAR_0 = 1$. As a result, the new pixel concentrations for the normalized image would generally fall between -1 and 1, which would make the function's following computation simpler. The normalized image of the minute fingerprint identification from the FVC 2000 DB and FVC 2002 DB datasets is shown in Fig. 6 and Fig. 7.

### 3.2.3. Binarization

Before beginning the process of extracting minutiae details, the improved fingerprint images need to be binarized. The enhanced fingerprint images are binarized before the process of obtaining fine information for detection. This process converts the input images from a multi-level grayscale to binary format, converting 8-bit grayscale image to 1-bit binary twin with ridge values of 0 and valley values of 1. Aspect extraction is also made easier by the approach, which significantly upsurges the contrast among the impression ridges and gorges. In this function, they classified two data levels such as the foreground ridge and the background valleys, which made up the binary image's output. In the Gabor filter grayscale image $E\,(i,j)$, which is provided by, binarization is possible by giving pixels with values greater than zero to one and pixels with DC components with a value of zero. In Fig. 8, binarized images of minutiae fingerprint images of the function are defined in Eq. (3).

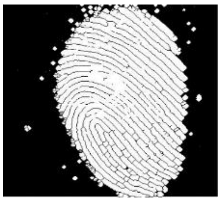

Figure. 9 Ridge thinned image of FVC 2000 DB

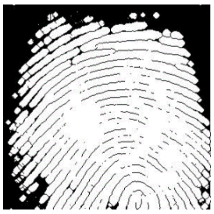

Figure. 10 Ridge thinned image of FVC 2002 DB

$$Binary\ (i,j) \begin{cases} 1, & if\ E(i,j)) \geq 0 \\ 0, & otherwise \end{cases} \tag{3}$$

### 3.2.4. Ridge thinning

Thinning is a method for reducing the fingerprint's ridge to a minimum of 8 distinct connected curves. It also works to get rid of as many superfluous pixels as possible, leaving each ridge with a single thick pixel that serves its intended function. The primary component of the thinning technique is the deletion of contour points from connected components to build the skeleton of related components in a fingerprint image. Therefore, finding the fingerprint ridge and doing a structural analysis of the system became easier. The ridge structures shouldn't be altered during the thinning process, and it's important to maintain the ridges' connectivity as well as other aspects like ridge ending and bifurcation points. Fig. 9 and Fig. 10 show the ridge thinning of the minutiae fingerprint identification of FVC 2000 DB and FVC 2002 DB datasets.

## 3.3 Fingerprint feature extraction:

After completing all of the aforementioned pre-processing steps, the enhanced fingerprint image is obtained, which can quickly find and recognize the small feature areas. An effective and reliable feature extraction technique is necessary for the final accuracy matching function. The methods based on minutiae-based aspects face issues related to the quality of the fingerprint samples, matching accuracy, computational complexity and processing time. Moreover, aspect based extraction algorithms are utilized to extract the required aspects from the images of fingerprints. In general, the function strengths of SURF, SIFT, BRISK, and accelerated-KAZE are to be used to demonstrate that they are the best solutions for object recognition. These categories were used to classify feature extraction algorithms. In this order, an improved A-KAZE and SURF algorithm combination was utilized. It has the potential to provide a set of features that are highly represented, repeatable, and have excellent matching properties.

### 3.3.1. The proposed A-KAZE - SURF algorithm:

Extraction played a key influence in the final accuracy and effectiveness of the fingerprint-matching procedure. Most of the existing fingerprint identification systems are based on the SURF algorithm to enhance fingerprint validation and the identical space regions are denoted through lines and regional boundaries of images. Therefore, the proposed accelerated- KAZE and SURF extraction procedure was carried out in this work with efficient repeatability and function-matching scores. The accelerated version of the KAZE, known as the A-KAZE, helps to shorten the time needed for feature extraction and the description of the identification process. Additionally, it exhibits less fluctuation in matching scores across incidence angles, which makes it ideal for the comparison of photos taken before and after a single block's activity. The A-KAZE feature detection was extracted using the Hessian matrix algorithm of $L_{xy}^{i}, L_{yy}^{i}$ and $L_{xx}^{i}$ are represented in Eq. (4).

$$L_{Hessian}^{i} = \sigma_{i,norm}^{2}\left(L_{xx}^{i}L_{yy}^{i} - L_{xy}^{i}L_{xy}^{i}\right), \qquad (4)$$

In where, $\sigma_{i,norm}^{2}$ was the normalized scale factor defined as $\sigma_{i.norm} = {}^{\sigma_i}/_{2^{o^i}}$ of the function. Additionally, the second, vertical, and horizontal lines are, $L_{xy}^{i}, L_{yy}^{i}$ and $L_{xx}^{i}$, respectively. In this case, when the current scale's value of Hessian extreme is higher than the pre-threshold, $T_A - KAZE$ , the Hessian algorithm is to be used to find the extreme points between the detected point in 3 × 3 × 3 neighborhood and the neighbor scales' 3 × 3 rectangle windows of the function. By performing a search around the radius of $6\sigma_i$ with sample steps of $\sigma_i$ to the KAZE characteristics were to be centralized in the system. Furthermore, in the first step, the Gaussian-weighted locations were performed at the differential values of all the nearby points in a circle to be centered. These value points are seen as the sector region of the image's pixel response value. After traversing the whole circle, the sector region with the highest value was supplied as the primary orientation for the function's aspect points. In addition, it creates a non-linear scale-space rather than applying Gaussian blurring and finds a very high number of inlier features in the function.

Speed up robust features (SURF) technique is robust to changes in illumination and affine translation in addition to being invariant to scaling and rotation. The descriptor creates the feature vectors of the identified key points of the function while the detector finds the key points and identifies their features. The main goal of the SURF discovery technique is to find areas of interest within a picture, such as angles or blob-like formations, where the element of the Hessian medium has a supreme value. Three tasks—key point detecting, key point characterizing, and key point matching—are performed during each step of the SURF algorithm. Initial stage is to detect the critical points of the given fingerprint image using the Hessian matrix $H(x;\sigma)$ which is represented in Eq. (5).

$$H(x;\sigma) = \begin{bmatrix} L_{xx}(x;\sigma) & L_{xy}(x;\sigma) \\ L_{xy}(x;\sigma) & L_{yy}(x;\sigma) \end{bmatrix} \qquad (5)$$

where; considering the image “i”, the medium $H(x;\sigma)$ is distinct at $H(x)$ and scale $\sigma$, which is presented in Eqs. (6–8).

$$L_{xx}(x;\sigma) = I(x) \times \frac{\partial^2}{\partial x^2}\, g(\sigma) \qquad (6)$$

$$L_{xy}(x;\sigma) = I(x) \times \frac{\partial^2}{\partial xy}\, g(\sigma) \qquad (7)$$

$$L_{yy}(x;\sigma) = I(x) \times \frac{\partial^2}{\partial y^2}\, g(\sigma) \qquad (8)$$

In this function where $L_{xx}(x;\sigma)$ is the image's second derivative of the Gaussian convolution, $g(\sigma)$ at scale $\sigma$. The Gaussian second-order derivative is simulated using the box filter to reduce computation time. The factors such as $D_{xx}(x;\sigma)$ , $D_{xy}(x;\sigma)$, and $D_{yy}(x;\sigma)$ are utilized in accelerating convolutional calculations by minimizing the processing time. Hessian's determinant's approximate value is calculated as shown in Eq. (9).

$$det\left(H_{approx}\right) = D_{xx}D_{yy} - (0.9\, D_{xy})^2 \qquad (9)$$

The first is to use the perpendicular and straight Haar wavelet strainers to convolve the feature pixel into its surrounding area to establish the orientation of each identified feature. The creation of a key point descriptor is done in step two of the system.

Additionally, KAZE exhibits less variation in the matching score across all incidence angles, which

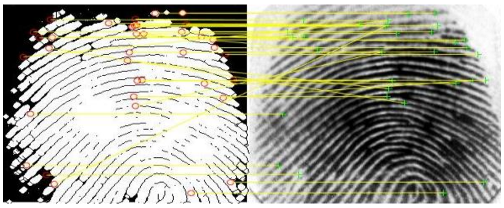

Figure. 11 Feature matching of the minutiae fingerprint image using FVC 2000 DB

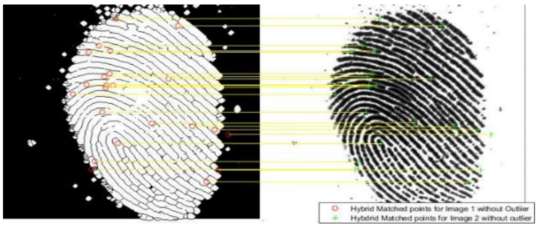
Hybrid Matched points for Image 1 without Outlier
Hybrid Matched points for Image 2 without outlier

Figure. 12 Feature matching of the minutiae fingerprint image using FVC 2002 DB

contributes to its effectiveness as an image-to-detection technique. A strikingly high number of inlier features are also detected by KAZE -SURF in contrast to other approaches, where the proportion of inlier corresponding aspects tends to rise with the number of corresponding aspects. More specifically, it demonstrated outstanding results for the translational and rotational components of the function in each disorder of the inter-frame, accrued point errors, and extracted gesture errors. The A-KAZE- SURF algorithm's final phase, which helps to improve aspects matching, involves computing a pairwise detachment among the aspects courses of the query duplicate and database images of the system.

## 4. Finger-print feature matching

The effective feature extraction matching procedure was required to identify the orientation opinion in a binary image and to find a corresponding opinion in another twin. The aspects of target regions in picture pairs were found using feature detection techniques, and features are similar to the identified features were matched using feature matching techniques. After removing the SURF aspects and computing the descriptors, geometrically dependable aspect matches are discovered across all impression images of the function. To correctly determine the matching area, we apply the (RANSAC) algorithm to recognize and eliminate opinions that are external at the beginning as outliers. The RANSAC algorithm's fundamental goal is to identify a model in which the data facts that best fit the model are retained and unfit points are removed. To create an index-pair matching matrix, the points based on collected from fingerprint pictures are associated with one another by utilizing the values related to proximities and Euclidean distance. To improve the score similarity of the inlier scores and the final accuracy of the function, the proposed KAZE-SURF with RANSAC matching algorithm was well utilized for the identification of minutiae impressions. It also provides high corresponding performance through high invariance, even for changes in scale, rotation, and partial affine image transformation of each feature in the image pairs. The feature-matching functionality of the minute fingerprint identification of the FVC 2000 DB and FVC 2002 DB datasets is shown in Fig. 11 and Fig. 12.

## 5. Similarity score calculation

After effective fingerprint matching, they need to calculate the similarity or matching percentage among the fingerprints. The process of matching is evaluated by computing the average value of the match score with pre-defined threshold value. At last, resemblance or corresponding percentage ($Pc$) is evaluated using the subsequent formulation as given in Eq. (10):

$$Pc = \frac{|CF|}{|TF|} \quad (10)$$

Where $TF$ is the total number of matching features in the system's index matching pair matrix and $CF$ is the number of correctly matching features (inliers) after the RANSAC algorithm has been applied. Additionally, taking into account the calculation of the similarity score, which improves the feature extraction of the inlier components from the minutiae details of the fingerprint image, and the matching features of the function Moreover, the similarity score is calculated as below in Eq. (11):

$$Similarity\ score\ \left(T_Q T_E\right) = \frac{count_{\ match}}{Count_{\ match} + Count_{\ unmatch}} \quad (11)$$

The function compares every row in the enrolled template of $T_E$ and if the best match row ($R_{match}$) if is not a match, $Counter$ , $Counter_{match}$ is increased by one as well ($R_{match}$) removed from the enrolled template ($T_E$ ) Otherwise, ($R_{match}$), the matched counter, is increased.

## 6. Result and discussion

The proposed method is tested using the dataset that was generated by FVC2000 DB1, FVC2002 and FVC 2004 datasets. The dataset is guaranteed to

Table 1. Recognition accuracy of A-KAZE-SURF with FVC 2000 DB1 with feature identification:

| Users | Recognized Samples | Accuracy (%) |
|---|---|---|
| 1 | 8 | 100 |
| 2 | 8 | 100 |
| 3 | 8 | 100 |
| 4 | 7 | 87.5 |
| 5 | 8 | 100 |
| 6 | 8 | 100 |
| 7 | 7 | 87.5 |
| 8 | 8 | 100 |
| 9 | 8 | 100 |
| 10 | 8 | 100 |
| Total | 78 | 97.5 |

Table 2. Recognition accuracy of A-KAZE-SURF with FVC 2002 DB1 with feature identification:

| Users | Recognized Samples | Accuracy (%) |
|---|---|---|
| 1 | 8 | 100 |
| 2 | 8 | 100 |
| 3 | 8 | 100 |
| 4 | 8 | 100 |
| 5 | 8 | 100 |
| 6 | 8 | 100 |
| 7 | 8 | 100 |
| 8 | 8 | 100 |
| 9 | 8 | 100 |
| 10 | 7 | 87.5 |
| Total | 79 | 98.75 |

include photos in formats like grayscale, jpg, and png, etc. The FVC2000 DB1, FVC2002 DB1 and FVC 2004 datasets serve as the basis for all testing and assessment activities. The results are created using the signal datasets and output images and the implementation of the proposed framework is implemented on MATLAB software. The suggested A-KAZE and SURF extraction algorithm depends on the correctness of the correction for accuracy, and it performs best with skew-free images of the function. The mentioned signal datasets are created and labelled manually as a component of a framework.

**Accuracy:**

It is defined as the ratio of number of recognized fingerprint to the total number of fingerprints and it is evaluated using the Eq. (12) as follows:

$$ACC = \frac{Number\ of\ fingerprint\ recognized}{Total\ number\ of\ fingerprint\ presented} \quad (12)$$

**Error rate:**

The error rate of the system is the ratio of the number of identified matches to the total number of images as presented in Eq. (13).

$$Error\ rate = \frac{Number\ of\ error\ matches}{Total\ number\ of\ images} \quad (13)$$

### 6.1 Performance analysis of enhanced A-KAZE and SURF algorithm

Here, is the performance of the minutiae fingerprint detection and Identification using FVC 2000 DB1 and FVC 2002 DB datasets of the function. In fingerprint identification, the improved A-KAZE and SURF achieve the effective fingerprint detect signal image classification accuracy of FVC 2000 DB at 97.51% and FVC 2002 DB at 98.75% datasets. From the results, it is known that the combined set of features provides better detection accuracy than the individual features. Additionally, the performance of the Improved A-KAZE and SURF methods helps to improve the effective detection and classification by using minutiae fingerprint images. The RANSAC extraction algorithm is used by images for effective classification and the detection of the function.

The performance of the enhanced A-KAZE - SURF method is analysed with different classifiers and with different feature selections. Moreover, the performance evaluation of two different minutiae fingerprint identification datasets with various classifiers is evaluated which is shown in Table 1, and Table 2 are shown the comparison of the various fingerprint identification with different accuracy features.

### 6.2 Comparative analysis

This section shows the comparative analysis of the improved A-KAZE- SURF minutiae fingerprint image identification. The datasets such as FVC 2000 DB1, FVC 2002 DB 1 and FVC 2004 are used to evaluate the efficacy of the proposed approach for an effective fingerprint image classification. Moreover, the performance of the proposed A-KAZE- SURF is compared with existing approaches suggested by Samy Bakheet [17], Amit Kumar Trivedi [20], Eain Ul Sehar [21] and Samy Bakheet [22] which is shown in table 3. From the analysis, it is known that Improved A-KAZE –SURF feature with RANSAC extraction provides better performance than others. For example, the accuracy of the proposed A-KAZE-SURF identification accuracy of FVC 2000 DB is 97.51%, FVC 2002 DB is 98.75% and FVC 2004 is 92.12% whereas the method proposed by Samy Bakheet [17] achieved 95% for FVC 2002 dataset and 92.5% for FVC 2000 DB1 dataset. Thus the proposed approach shows effective detection and classification of the minutiae fingerprint identification. The better result of the proposed approach is due to A-KAZE and SURF extraction algorithm which helps to reduce the time required for feature extraction and the identification process.

Table 3. Comparative analysis of the Existing Recognition accuracy FVC 2000 DB1, FVC 2002 DB1 and FVC 2004 datasets

| **Methods** | **Datasets** | **Recognition accuracy(%)** | **Elapse time (s)** | **Equal error rate (ERR)** |
|---|---|---|---|---|
| Samy Bakheet et al [17] | FVC 2000 DB1 | 92.5 | 4.03 | NA |
| | FVC 2002 DB1 | 95 | | NA |
| Amit Kumar Trivedi [20] | FVC 2000 DB1 | NA | NA | 6.15 |
| | FVC 2004 DB1 | NA | | 2.24 |
| Eain Ul Sehar [21] | FVC 2002 DB1 | 94.05 | NA | 5.95 |
| Samy Bakheet [22] | FVC 2004 | NA | 0.674 | 02.01 |
| The Proposed A-KAZE-SURF method | FVC 2000 DB1 | 97.5 | 3.09 | 2.5 |
| | FVC 2002 DB1 | 98.75 | | 1.25 |
| | FVC 2004 | 92.12 | 4.35 | 01.70 |

From Table 3, it is observed that the proposed method achieved better results compared to the existing methods in terms of recognition accuracy, elapse time, and error rate. As detection accuracy is the major aspect to focus, the proposed methodology has highly driven on achieving better recognition accuracy. For instance, the proposed method achieved better recognition accuracy, high elapse time, and low error rate compared to other existing method like Samy Bakheet [22]. This method has low elapse time compared to the proposed method, however the recognition accuracy is unknown and also has high error rate compared to proposed method.

## 7. Conclusion

This research focused on the detection and classification of fingerprints and fingerprint images in a precise manner. In this research, different algorithms are proposed to effectively detect the matching fingerprint and un-matching fingerprint images of the function. The A-KAZE is an enhanced phase of KAZE that helps to reduce the time required for extracting the features of the identification process. RANSAC algorithm offers better efficiency while computing the images with higher invariance and transforming every individual feature of the image pairs. By utilizing these feature values, the irregularity and ordinariness of minutiae fingerprint disease were extracted using the RANSAC extraction algorithm. The identification results obtained were evaluated using measures such as recognition accuracy, elapsed time, and the error rate of the system. The proposed method showed improvement in the accuracy of identification FVC 2000 DB at 97.51%, FVC 2002 DB at 98.75% and FVC 2004 at 92.12% along with effective detection and classification of the minutiae fingerprint identification. The future work will be based on using various feature extraction methods to improve detection accuracy.

## Conflicts of interest

The authors declare no conflict of interest.

## Author contributions

For this research work all authors' have equally contributed in Conceptualization, methodology, validation, resources, writing—original draft preparation, writing—review and editing.

## References

[1] R. Gupta, M. Khari, D. Gupta, and R. G. Crespo, "Fingerprint image enhancement and reconstruction using the orientation and phase reconstruction", *Information Sciences*, Vol. 530, pp. 201-218, 2020.

[2] F. Pandey, P. Dash, D. Samanta, and M. Sarma, "ASRA: Automatic singular value decomposition-based robust fingerprint image alignment", *Multimedia Tools and Applications*, Vol. 80, No. 10, pp. 15647-15675, 2021.

[3] Z. Zhang, S. Liu, and M. Liu, "A multi-task fully deep convolutional neural network for contactless fingerprint minutiae extraction", *Pattern Recognition*, Vol. 120, p. 108189, 2021.

[4] S. Lee and I. R. Jeong, "Improved fingerprint indexing based on extended triangulation", *IEEE Access*, Vol. 9, pp. 8471-8478, 2021.

[5] Q. N. Tran, and J. Hu, "A multi-filter fingerprint matching framework for cancelable template design", *IEEE Transactions on Information Forensics and Security*, Vol. 16, pp. 2926-2940, 2021.

[6] N. Alay and H. H. A. Baity, "Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits", *Sensors*, Vol. 20, No. 19, p. 5523, 2020.

[7] B. K. Singh, R. Kumar, and R. R. Kishore, "A biometric system design using finger knuckle biological trait", *Multimedia Tools and Applications*, Vol. 81, No. 26, pp. 36835-36852, 2022.

[8] B. Ramkumar, R. S. Hegde, R. Laber, and H. Bojinov, "GPGPU acceleration of the KAZE image feature extraction algorithm", *arXiv preprint arXiv:1706.06750*, 2017.

[9] K. M. O. Nahar, B. A. A. Huda, A. F. A. Bataineh, and R. M. A. Khatib, "Twins and Similar Faces Recognition Using Geometric and Photometric Features with Transfer Learning", *International Journal of Computing and Digital System*, Vol. 11, No. 1, pp. 129-139, 2022.

[10] R. G. Martin and R. S. Reillo, "Wrist vascular biometric recognition using a portable contactless system", *Sensors*, Vol. 20, No. 5, p. 1469, 2020.

[11] R. G. Martin and R. S. Reillo, "Vein biometric recognition on a smartphone", *IEEE Access*, Vol. 8, pp. 104801-104813, 2020.

[12] D. M. Uliyan, S. Sadeghi, and H. A. Jalab, "Anti-spoofing method for fingerprint recognition using patch based deep learning machine", *Engineering Science and Technology, an International Journal*, Vol. 23, No. 2, pp. 264-273, 2020.

[13] T. Vijayakumar, "Synthesis of palm print in feature fusion techniques for multimodal biometric recognition system online signature", *Journal of Innovative Image Processing (JIIP)*, Vol. 3, No. 02, pp. 131-143, 2021.

[14] H. Ma, N. Hu, and C. Fang, "The biometric recognition system based on near-infrared finger vein image", *Infrared Physics & Technology*, Vol. 116, p. 103734, 2021.

[15] M. Baskar, R. R. Devi, J. Ramkumar, P. Kalyanasundaram, M. Suchithra, and B. Amutha, "Correction to: Region Centric Minutiae Propagation Measure Orient Forgery Detection with Finger Print Analysis in Health Care Systems", *Neural Processing Letters*, Vol. 55, No. 1, pp. 33-34, 2023.

[16] O. L. González, E. F. F. Mehnert, A. Morales, J. Fierrez, M. A. M. Pérez, and R. Monroy, "Impact of minutiae errors in latent fingerprint identification: assessment and prediction", *Applied Sciences*, Vol. 11, No. 9, p. 4187, 2021.

[17] S. Bakheet, A. A. Hamadi, and R. Youssef, "A Fingerprint-Based Verification Framework Using Harris and SURF Feature Detection Algorithms", *Applied Sciences*, Vol. 12, No. 4, p. 2028, 2022.

[18] Y. Surajkanta and S. Pal, "A Digital Geometry-Based Fingerprint Matching Technique", *Arabian Journal for Science and Engineering*, Vol. 46, No. 4, pp. 4073-4086, 2021.

[19] S. Aleem, P. Yang, S. Masood, P. Li, and B. Sheng, "An accurate multi-modal biometric identification system for person identification via fusion of face and finger print", *World Wide Web*, Vol. 23, No. 2, pp. 1299-1317, 2020.

[20] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "A Novel Minutiae Triangulation Technique for Non-invertible Fingerprint Template Generation", *Expert Systems with Applications*, Vol. 186, p. 115832, 2021.

[21] E. U. Sehar, A. Selwal, and D. Sharma, "FinCaT: a novel approach for fingerprint template protection using quadrant mapping via non-invertible transformation", *Multimedia Tools and Applications*, Vol. 82, pp. 22795–22813, 2023.

[22] S. Bakheet, S. Alsubai, A. Alqahtani, and A. Binbusayyis, "Robust Fingerprint Minutiae Extraction and Matching Based on Improved SIFT Features", *Applied Sciences*, Vol. 12, No. 12, p. 6122, 2022.

[23] Fingerprint Verification Competition FVC2000. Available online: http://bias.csr.unibo.it/fvc2000/

[24] Fingerprint Verification Competition FVC2002. Available online: http://bias.csr.unibo.it/fvc2002/

[25] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third fingerprint verification competition", In: *Proc. of Biometric Authentication: First International Conference, ICBA 2004, Hong Kong, China*, pp. 1-7, 2004.