iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39570

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Multifactor Authentication in Automated Teller Machine

Vigneshwar Muriki
Computer Science and Engineering, Sri Venkateswara University College of Engineering

Abstract: ***Skimming of card details is the primary problem faced by many people in today's world. This can be done in many ways. For instance, a thief can insert a small device into the machine and steal the information. When a person swipes or inserts a card, the details will be captured and stored. This problem can be solved using biometrics. Biometrics include fingerprint, iris, face, retina scanning, etc. This paper focused on solving this issue using fingerprint and iris recognition using OpenCV and propose a suitable method for this issue. Fingerprint and iris recognition are performed by identifying the keypoints and descriptors and matching those with the test data.***

Keywords: Biometrics, Fingerprint recognition, Iris recognition, Scale Invariant Feature Transform, Oriented FAST and Rotated BRIEF, OpenCV

I. INTRODUCTION

Biometrics springs from the Greek word bio meaning life, and metric meaning aspiring to measure. Biometrics is named analysis of individuals which supports their physical characteristics and measurement of their features. This technology is especially used for identifying people supporting their physical measurements. Authentication is another term meaning providing security systems to people and biometric verification.

Biometrics are accustomed to authenticating an individual regardless of age, sex, and physical appearance. Biometrics can enhance security and reduce problems associated with skimming. Now-a-days most electronic devices like mobile phones, computers, and other devices can automatically open after they detect the fingerprints and iris of a user and there is also no phone without fingerprint recognition.

The benefits of biometrics [1] include providing high security and assurance. There are many types of biometrics like fingerprint recognition, iris recognition, automatic face recognition, retina scanning, etc.

Fingerprint recognition [2] is the method where we compare two fingerprints of an individual and check whether their fingerprint match. This method is used specially to verify a person's authenticity. The rationale why fingerprint recognition is in ATMs is that it is easy to use and is flexible to put in. Fingerprints do not change throughout your time although we get older or aged the fingerprint remains identical, but when people are aging it will be difficult to read the fingerprint because they're going to lose collagen.

Fingerprints are the marks impressions made on the surface by a person's fingertip[3]. Fingerprints reveal a lot about a person like their intelligence, personality, talents, etc. Every individual has a unique fingerprint structure and does not match with any other individual. It consists of ridges, bifurcation, ridge ending, crossover, island, core.

1) *Ridge:* Curved lines in a fingerprint.
2) *Ridge Ending:* Some ridges are not continuous curves. They terminate at some specific points. Those points are called ridge endings.
3) *Bifurcation:* Point where a ridge forks or diverges into branch ridges.
4) *Core:* This is the centre part of the fingerprint.
5) *Crossover:* It is a connecting friction ridge made up of two bifurcations.

Iris is the coloured portion of the eye that regulates the size of the pupil[4]. It separates the two regions of the eye. The sclera is the white part of the eye that surrounds the cornea. The iris controls the amount of light entering the eye by contracting and relaxing the eye muscle.

Iris recognition [5] is identical to fingerprint recognition where within the place of fingerprint we match the iris of an individual. Iris is a unique coloured circle a part of our eye which we scan the iris first and so match it with the iris stored within the database. Iris recognition [6] is understood for its accuracy because no two persons can have an identical iris and the iris may not be skimmed or stolen.

II. METHOD

Both fingerprint and iris recognition follow similar steps. The only difference is the algorithm that is used to find the similarities between the two images. The modeling is performed by loading the dataset. We used *OpenCV* to find keypoints and descriptors in both fingerprint and iris using *SIFT* and *ORB* algorithm.

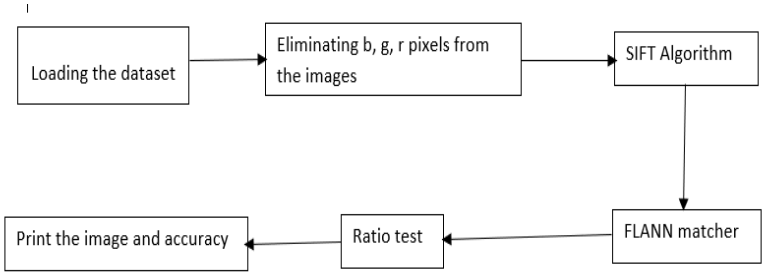


Figure 1: Flowchart for fingerprint recognition

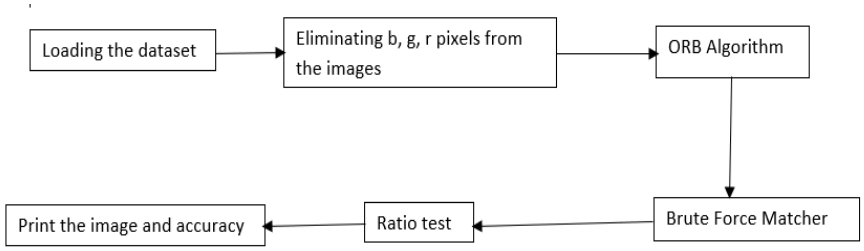


Figure 2: Flowchart for iris recognition

For fingerprint recognition, Fast Library for Approximate Nearest Neighbours (*FLANN)* matcher was used to find matches between the two images. In general, this is used for larger datasets. For iris recognition, Brute Force (BF) Matcher was used to find matches between images because the dataset is small. In the final step, we use matplotlib for plotting images and find the best matches.

Initially, the images are tested to whether they have the same shape and channels. If they have the same size and channels, we can split them into three RGB channel images. Now we count the number of non-zero pixels. We eliminate the *b, g, r* pixels from the image. From here the implementation changes for both fingerprint and iris.

In fingerprint recognition, we use Scale Invariant Feature Transform (SIFT) algorithm for detecting keypoints and descriptors. In the next step, FLANN matcher was used. It contains a collection of algorithms optimized for nearest neighbours search in large datasets and high dimensional features. Inside the FLANN, two dictionaries namely index, and search parameters are passed which specifies the algorithm to be used. Further, good keypoints are generated using a ratio test. Good keypoints are considered based on the distance between the descriptors. Lower the distance between them, the better it is. Using the distance constraints, keypoints are generated. The total number of keypoints generated will be greater than the two keypoints obtained from two images. Based on the number of keypoints obtained, keypoints are generated in both images and accuracy is obtained.

For iris recognition, ORB algorithm was used. Like SIFT algorithm, keypoints and descriptors are generated for both iris images. Since the dataset is smaller, BF Matcher was used. Using some distance calculation, the descriptor of the image in the real data is matched with all the images in train data and the closest one is returned.

BF Matcher takes two optional parameters. Out of which the first one is normType which specifies the distance measurement to be used. By default, it is *cv2.NORM_L2.*

The second parameter in BFMatcher is *crossCheck*. By default, it is *false*. If it is true, the matcher returns only those matches such that i^{th} descriptor in real data has j^{th} descriptor in train data as the best match and vice versa. It provides consistent results and a good alternative to ratio test used in *SIFT* algorithm.

Then we sort the matches in ascending order of their distances so that the best matches with low distance come to the front. Images are stacked horizontally, and lines are drawn from the first image to the second image indicating the best matches. Initializing flags=2 means that draws two-match lines for each keypoint.

III.RESULTS

Each image is tested with the images in train data and returns the fingerprint with the best matches. In Figure 3 there are some common keypoints between the two fingerprint images. But there was no line-to-line matching between the images. Though the below two images have the same size and channels, they are not completely equal.

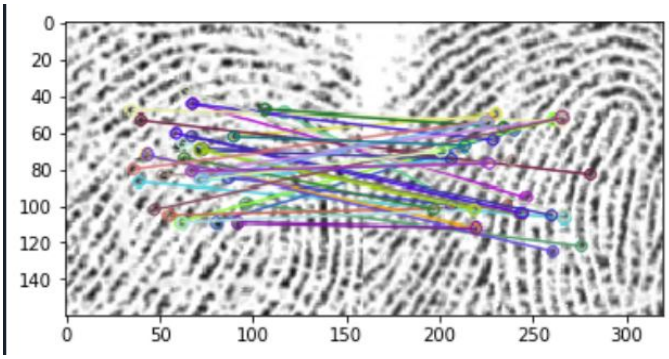


Figure 3: Irregular keypoint matching

Figure 4 depicts the exact keypoint matching between two images.

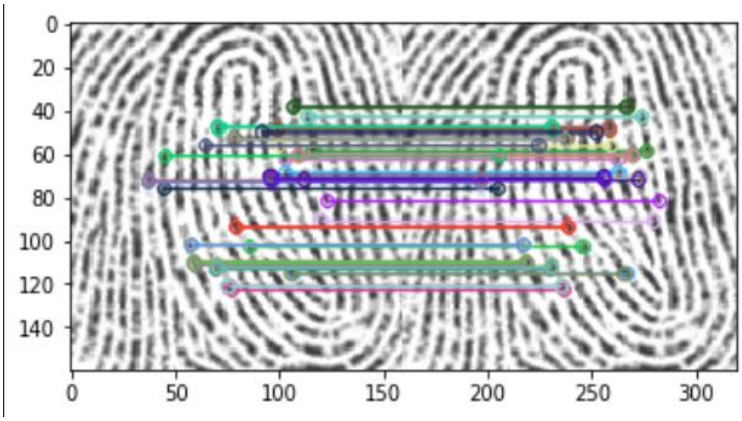


Figure 4: Exact matching of keypoints

Out of 800 images in the train data, three images from the real data matched with the images in train data. The average accuracy is found to be 98%.

In iris recognition, the training data contains 200 images and test data contains eight iris images. Similar to fingerprint recognition, if there is a line-to-line matching of keypoints then they are said to be same and returns the maximum accuracy.
Below figure explains the same.

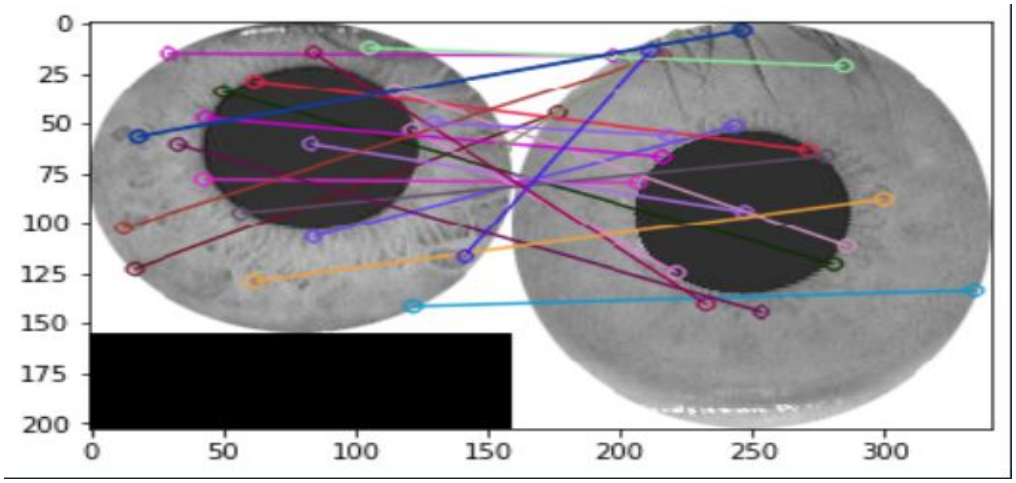


Figure 5: Irregular matching of keypoints in iris

In the below image,we can see accurate keypoint matching in both the images.

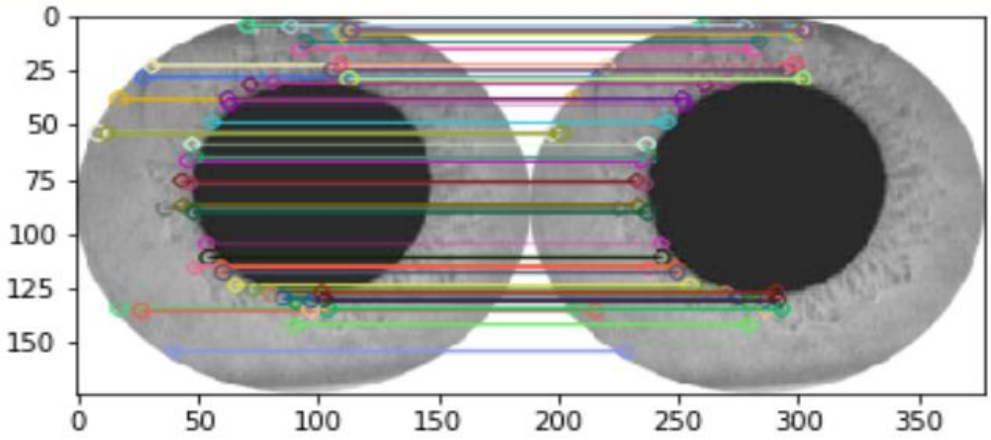


Figure 6: Accurate matching of keypoints in iris

Out of eight images in the real data three images matched with the images in the database. Table 2 depicts the accuracy between iris images. The average accuracy is 99.5%

IV. CONCLUSION AND FUTURE WORKS

Based on the results obtained from both fingerprint and iris images, iris recognition is considered as the best recognition system as maximum average accuracy is attained and it is impossible to copy iris of others and iris does not change with aging. The above-proposed implementation works to some extent. As the size of the database increases it will be become much slower to authenticate an identity.

Future works include a detailed implementation of fingerprint and iris recognition and other biometrics. Both implementations can be done further using hardware. There had been cases where fingerprint scanners are fooled by digitally modified or partial images of fingerprints [7]. To improve security [8], we can introduce an embedded crypto-Biometric authentication scheme for banking systems [9]. Cryptography and biometric techniques are used for person authentication to improve security levels.

REFERENCES

[1] "Biometrics and identity fraud protection: Two barriers to realizing the benefits of biometrics – A chain perspective on biometrics, and identity fraud – Part II - ScienceDirect." https://www.sciencedirect.com/science/article/abs/pii/S026736490500097X (accessed Dec. 21, 2021).

[2] "A minutia-based partial fingerprint recognition system - ScienceDirect." https://www.sciencedirect.com/science/article/abs/pii/S0031320305001445 (accessed Dec. 21, 2021).

[3] "Fingerprint," Wikipedia. Oct. 20, 2020. Accessed: Oct. 25, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Fingerprint&oldid=984451165

[4] "Iris Anatomy of the Eye, Pictures & Definition | Body Maps," Healthline, Jan. 20, 2018. https://www.healthline.com/human-body-maps/iris-eye (accessed Oct. 25, 2020).

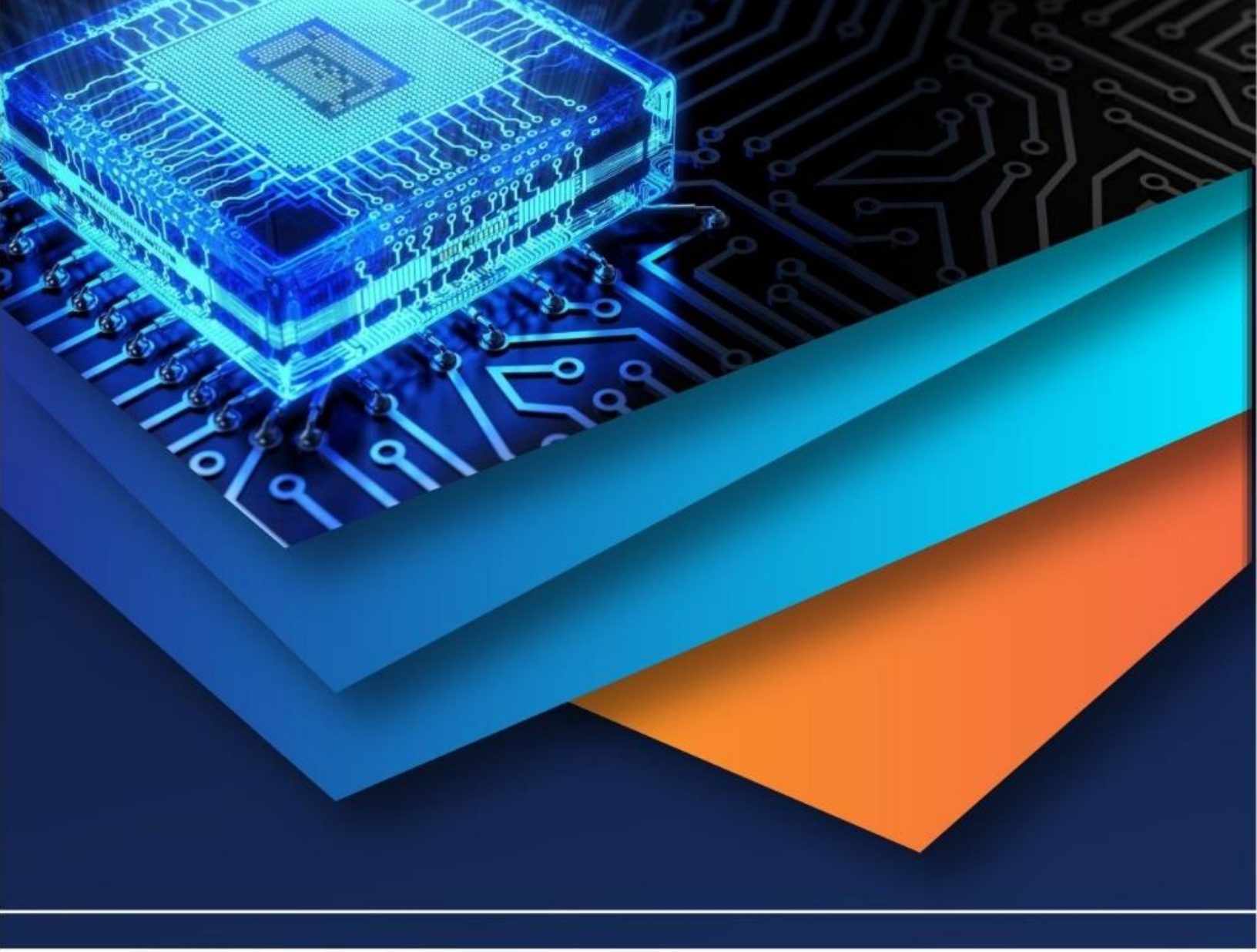
[5] "How Iris Recognition Works - ScienceDirect." https://www.sciencedirect.com/science/article/pii/B9780123744579000251 (accessed Dec. 21, 2021).

[6] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Efficient iris recognition by characterizing key local variations," IEEE Transactions on Image Processing, vol. 13, no. 6, pp. 739–750, Jun. 2004, doi: 10.1109/TIP.2004.827237.

[7] "https://www.marketwatch.com/story/heres-how-easily-hackers-can-copy-your-fingerprints-2017-05-25%20(accessed%20Oct.%2007,%202020)," MarketWatch. https://www.marketwatch.com/story/heres-how-easily-hackers-can-copy-your-fingerprints-2017-05-25%20(accessed%20Oct.%2007,%202020) (accessed Dec. 21, 2021).

[8] "IJRST-016.pdf." Accessed: Dec. 21, 2021. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/33380857/IJRST-016.pdf?1396545426=&response-content-disposition=inline%3B+filename%3DUsing_Advanced_Encryption_Standard_AES_A.pdf&Expires=1640109235&Signature=E8HlGcELMcZvT639-I5QQlxvMT2ZNQMWoXDUJDc7Cq7blUMdZUO0PH0pFprRVKSMF9b9CGb2SImWmh3qBbqboPdjsRmf-GRy2QV6BgV~olfWK2jzzHQ5bMEYHM7T4epwCHS5A9aPVldCQ1ka4Kzudl~9HYjZPxSFX9JKdqS2ILkS35-pSEsoijmeCQl6hodEX0bRq3gIqhMBVbsB7xn3Y009zyHFhZR2lFw7~fnYr0CP7M15xtUx8HOzltmjA17LZ8JPxvt9VZS4TtSeEQuW2amxsuaGId8MDwA8XPdMypiR2tZIw4nqLrwwdndCHxlxYmQvzghp3gMjMn~GtpnpiQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[9] "Cryptographic Keys with Android Fingerprint Authentication," ArcTouch. https://arctouch.com/blog/cryptographic-keys-fingerprint-authentication-android/ (accessed Dec. 21, 2021).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY