A DIGITAL SMART VOTING SYSTEM USING FINGERPRINT AUTHENTICATION AND FACIAL DETECTION ON CNN AND IMAGE PROCESSING

[1]Y.Susheela, [2]Dr.Dinesh Kumar, [3]Dr. N. Chandra Mouli
[1]Assistant Professor, [2,3]Associate Professor, [1,2,3] Dept. of Computer Science Engineering,
[1,2,3]Vaageswari College of Engineering, Karimnagar, Telangana.
E-Mail: chiduralasusheela@gmail.com, sahni.dinesh@live.com, cmnarsingoju@gmail.com

ABSTRACT
India is a democratic nation, yet it continues to use expensive, labor-intensive voting machines to conduct its elections. Voters can cast their ballots using the web-based method from anywhere in the world. For use in the online election, the Indian government created a restricted IP address. For the purpose of registering names and addresses, people should visit the website. The election commission will take fingerprints and a photo of each voter. The images will be kept on a server or in a database. Election Day voting is secure because to a database comparison performed when the pictures are obtained on that day. Similar to how mobile phones operate, faces and fingerprints are utilized to access the voting process. The existing system necessitates voter physical presence, which many voters find inconvenient. In addition, the procedure takes less time. The number of bogus voters can be minimized by detecting facial and fingerprint images. To make the system safer, the space between the eyes and the eyebrows remains consistent with age.
Keywords: Online website voting, face capture, Haar cascade face recognition, fingerprint, image pre-processing, Convolutional Neural Networks (CNN).

INTRODUCTION
Elections are the cornerstone of any democracy, and when people elect their own government, democracy is truly alive. However, there are weaknesses and gaps in the way our country now conducts elections that candidates and political parties are taking advantage of. The current system has many faults, including the possibility of voting twice, manipulating Electronic Voting Machines (EVMs), and falsifying the results, all of which undermine democracy in its truest form. Elections are typically conducted using electronic machines, which is labor- and energy-intensive, and should be done at a designated area. The machine is expensive and takes more labor to move and maintain. The approach proposed here is a solution that covers all of the issues raised. People who do not live in the same area, the elderly, or those who cannot wait in huge lines for long periods of time will benefit from the Smart voting system, which uses facial and fingerprint identification. The voter can vote from anywhere, and the possibility of duplicate votes is reduced as a result. Using haar Cascade Algorithm, this online voting system employs image processing to detect voter faces[1] .
To extract the lips, face, and eyes from a whole face and compare them to a database image of a face. The image of a fingerprint is matched using CNN Deep Learning. CNN reduce the computational time for processing the large size images[2]. The Artificial Neural Networks (ANN) training takes a long period. Future detection and picture classification are two steps of CNN. The features of face and fingerprint images are measured and compared to the database. When it's the same, the voter will be permitted to vote. In an election, voters can vote for any candidate. After that, the additional leader slots will be disabled. The votes are recorded on a server, and the counting is completed at the conclusion of the election. Client and server commission are critical to the system's success[3].
The Internet Protocol (IP) address is obtained from the election website of the government. After the crucial information is provided to the system to separate the eligible voters from the false ones, counting is very simple

and takes very little time compared to the present system. Importantly, the system designed is totally web-based, making it very cost-effective in comparison to current methods. In addition, if the website is properly secured, very little staff will be required. Existing systems, as well as being an authentic model[4].

LITERATURE SURVEY

Iris Detection in Voting System

The image of the eyes is taken, and the Iris is recognized and compared to the stored photographs using image processing techniques. When it matches, the system verifies that the voter is permitted to vote by validating his or her Aadhar data. The voter will be able to vote once their identity has been verified. [5] Because the existing Aadhar database contains all of the information regarding a voter's iris, fingerprints, and other personal information like as address, a blood-group voter can be easily tracked and verified[5]. This method takes less effort and is quitesafe.

Fingerprint Recognition Voting System

Fingerprints are recognized by a sensor and stored in a database. The information fromthe biometric image will be transferred to the web application via the serial port of the microcontroller[6]. The voter's identification is confirmed when the input image is compared to an existing image in the database, or when the server sends the message and displays it on the Liquid Crystal Display (LCD). If there are no matches, the LCD displays "not eligible." [2]

Smart Voting

Individuals above the age of 18 will have their information obtained from the Aadhar database. During the initial stage, before the voting procedure, the voters will receive an Id and password via their registered email address. [7] The voter's identity is verified using fingerprint data in the second step, and the voter is then permitted to vote. The voter id will be removed aftercasting the vote as part of the third step, thus there will be no opportunity to vote again. The voter's Aadhar details will be locked, allowing the voter to be tracked for future access. Thecount will be updated in parallel.

Block chain Based Secure Voting System using IOT.

The voting process is documented in the client and saved in the server [5]. The voter's name and address are entered into the website, and the voter is assigned a number during the voting process. A sensor is used to capture a fingerprint image, which is then compared to database photos. When it matches the input, the voter is given the option to vote[11. The term "block chain" refers to voting blocks that are recorded for each voter and saved on the server.

CNN-based Multimodal Biometrics

Multimodal Biometrics is a new technology that secures photographs of the face, iris, and palm print. Convolutional Neural Networks were used to extract image features. Multimodal Biometrics is an old method that employs CNN. Using CNN, the input image is compared to images in the database. CNN is also in responsible of fingerprint image matching. In the most recent CNN, two layer fusions were used [13].

PROPOSED SYSTEM

Face and fingerprint recognition is used in the created and proposed smart voting system. It is more secure than current systems because it uses image processing and CNN. The most important level of security is when the system recognizes a voter's face and fingerprint from an existing database of Election Commission face and fingerprint photos. If the image obtained matches the image of the voter in the database, the voter is eligible to vote[15. The Hair Cascade algorithm is used to extract facial features and detect facial parts of an image. Visual Studio and HTML tools were used to build the web platform and implement the algorithms. Feature point-based collation methods are used to collate fingerprint photos with images from the Election Commission. If the resulting images match, the voter will be given the opportunity to vote.

METHODOLOGY

Because this concept is totally web-based, the primary characteristics are web-based technologies such as database generation and image processing qualities, which dictate thesystem's software requirements. This is a list of official government websites. Voters will be ableto utilize this website to cast their ballots. After facial and fingerprint recognition, eligible voters will be allowed to vote. On election day, the voter will access the website. Fingerprints and face photographs are stored in server that had been authorized by the Election Commission. With the IP address provided, voters can access the website. When a voter opens the website and clicks the vote button, their face and fingerprints will be photographed using whatever device they are using to access the website, such as a laptop, PC, or their mobile camera. The server will then getthe captured image. The server searches through all of the photographs in the database for a match in the ones that have been registered. If the voter's face and fingerprints match, the election commission will register and identify him or her, allowing them to vote. The Haar Cascade method is used to recognize faces. If no match is detected, the page will state that the voter is not recognized and that they will not be able to vote. When the fingerprint images are identical, the server saves the fingerprint image. The ten fingerprint images are captured, and the ten finger's position and count are calculated. We can determine the correct voter fingerprint by comparing the two photos. The input and picture saved in the database are compared using CNN to match fingerprint images. The photos that have been matched will be presented together with their ID numbers, as well as a voting website where voters can vote for any political party from alist of voter selections[16]. When they select their favorite party, the option cannot be modified, and the rest of the options are also disabled. The server accepts and saves the votes cast by verified voters. The number of votes cast for each political party's candidates will also be recorded. Even the counting of votes is simplified in this fashion, and the mission, candidates, and voters do not have to wait days for the results.

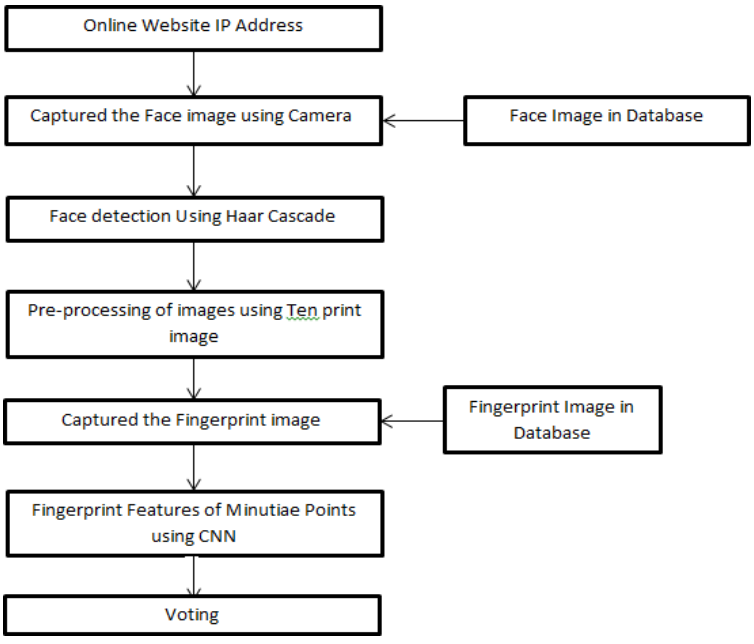


Fig. 1 Methodology of the System

HAAR CASCADE FOR FACE DETECTION

Object detection, often known as face detection, is a technique for identifying things in aphotograph or video. The Haar features-sequence of square-shaped functions is used to train the algorithm to detect a face. Then it

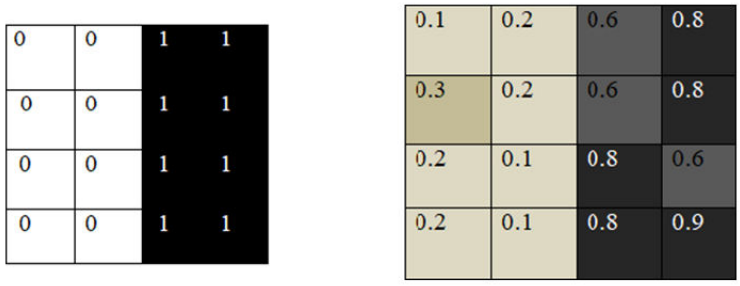
employs classifiers to determine whether or not there is a face [1]. There are four phases to face detection. The

first stage involves detecting Haar features using integral pictures, the third stage involves Adaboost, and the fourth stage involves a classifier cascade.

Fig.2. Face Detection

Detecting Haar characteristics

Prior to Haar features, image pixel intensities were employed for face detection, which required a great deal of effort and time. Instead, Haar wavelets detect faces by computing thesum of their pixel intensities and then the difference between these sums. We have adjusted grey scale for black and white image pixels[17].



(a) (b)

Fig. 3 Pixel intensities of detected Haar-features (a) ideal case (b) real case.

Detecting Haar feature in the image

$$\Delta = \frac{1}{n}\sum^{n}(x)_{dark} - \frac{1}{n}\sum^{n}(x)_{white} \quad \text{Eq.(1)}$$

Ideal case:
$$\Delta = \left(\frac{1}{8} * 8\right) - \left(\frac{1}{8} * 0\right) = 1$$

Real case:
$$\Delta = \left(\frac{1}{8} * 5.9\right) - \left(\frac{1}{8} * 1.3\right) = 0.575$$

Haar features are particularly good at detecting rectangular characteristics, making it a useful face detection tool. Figure 3(b) shows a possible eye. The darker area corresponds to the eye, while the lighter area corresponds to the cheek area of the face. Eyes are recognized first because they are the darkest regions of the face in comparison to the rest of the face, whether in grey scale photos or otherwise. Figure 3(a) shows how the bridge of the nose is usually higher and darker than the cheek area of the face. This is how Haar features detect the face or subsections of the face first while detecting lines and edges.

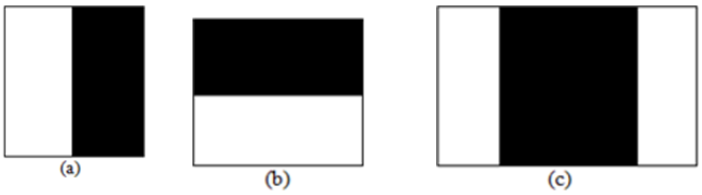
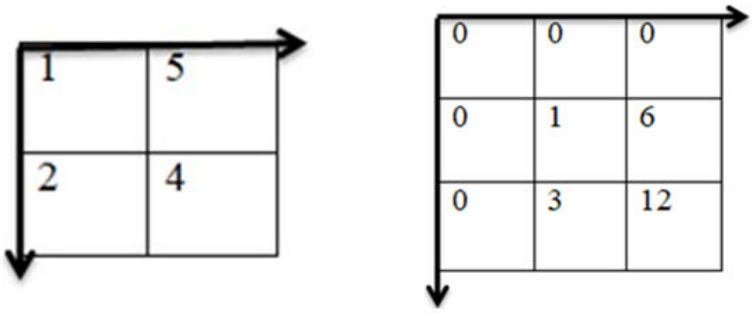


Fig.4.Some common Haar features (a) Nose (b) Eyes (c) Mouth.

Integral images

Haar features are especially useful as face detection tools because they are particularly good at detecting rectangular features. Figure 3 (b) shows the possible eyes. The dark areas correspond to the eyes and the bright areas correspond to the cheek areas of the face. The eyes are first detected because they are the darkest areas of the face compared to the rest of the face, whether in gray scale or not. Figure 3 (a) shows that the nasal bridge is usually higher and darker than the cheek area of the face. In this way, hair features first recognize the face or facial subsections, and lines and edges are recognized. If you consider the following boxes as a subset of faces, the numbers represent pixel intensities. The table on the left should be 1 + 5 + 2 + 4, which is equivalent to 12. On the right is a table containing cumulative totals by row and column. Here you need to enter 12 + 000, which is equal to 12. We've seen simple calculations here, but as the subset grows, calculations using integer images become much faster, less time consuming, and more effective.



(a) (b)

Fig.5.The Generated subsets of a grid (a) input image (b) integral image

Adaboost

Features, in addition to being numerous, may also be irrelevant. A feature that is a component of one's appearance. Adaboost determines the best and worst features, as well as the classifiers that employ them. The method creates strong classifiers and 'weak' classifiers. Astrong classifier has a lower error rate, indicating that it will almost certainly be a feature of the face, whereas a 'weak' classifier has a lower error rate, indicating that it will almost certainly be afeature of the face.

As a result, we use Adaboost to combine several weak classifiers into a single strong classifier that can recognize faces.

Cascade of classifiers

There are face-regions and non-face-regions in an image. The features extracted from subsections are fed into various stages of classifiers. The remaining features are not taken into account. The second step of features will be added, and the process will only proceed if the first stage is passed. The window that crosses through each stage is the required face region. Cascade is employed in order to save time, energy, and effort at all stages. Only the face feature will be detected by the window. The cascade of classifiers has no place in the face region; the phases merge to form one large window, resulting in the detected face.

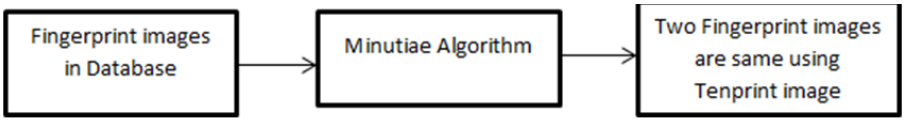
IMAGE PRE-PROCESSING WITH TENPRINT

We can utilize the ten print image approach when the two fingerprint pictures are identical. For each fingerprint image in the database, ten fingerprint images are captured and features are stored. We'll go over each of these traits in turn in this part, with the tiniest attributes gettingtheir own section. When two people's fingerprints are identical and their records have the same value. A physical finger position has been assigned to the ten print image mate minutiae records, as well as all image records in this database.

The fingerprints of two voters are identical, and minor details are recorded. These characteristics include ridge endings, which are spots in a finger's friction.

An automatic AFIS system initially spotted the perfect minutiae on the ten print image mate. Using a combination of ten fingerprint images and features recorded by minutiae points, the two features of fingerprint images were compared to determine which voter was accurate.

Block Diagram of Ten print image



Algorithm for ten print images:-

The first step is to take the input image.

Step 2: Image Binarization: A grey image is turned to a binary image in this step.

Step 3: Image thinning: To remove unnecessary pixels and train the algorithm

Step 4: When two fingerprint photos in the database are identical. Tenprint photos are used.

Step 5: A total of ten fingerprint photos are taken, and the location of the fingers, as well as therecord and count, are determined.

Step 6: The latent image is compared to the database's Tenprint image.

FINGERPRINTS RECOGNITION USING MINUTIAE CNN DeepLearning

The voter's fingerprint is captured by the sensor and stored in the database. The fingerprint of the input device is compared to the fingerprint provided by the Election Commission. Fingerprint recognition can be used to verify the authenticity of your fingerprint. A person's fingerprint is used to confirm the vote. Feature points and fingerprint matching Deep learning and machine learning are not the same. Machine training takes a long time, but deep learning is quick and less expensive than machine learning.

Fingerprint images Matching with minutiae CNN

The fingerprint is scanned and stored in the database using a sensor. Another input is providedto CNN, which compares two fingerprints and provides picture features.

CNN determine minutiae points in Dv =(S1,S2)

Fingerprint matching is likewise done in CNN by comparing the minutiae points of Dvfingerprints.

Basics of CNN

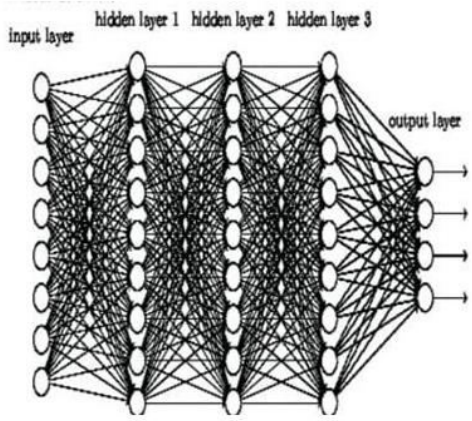


Fig.6. Block Diagram of CNN

1) CNN includes a convolutional layer as well as filters, and it is paired with ANN.
2) The use of a convolutional neural network was reduced. The processing speed of a hugeimage is slowed.
3) The input image size is 128*128, while the output image size is 5*5.
4) ANN is a weighted algorithm that takes several minutes to train.
5) CNN has been taught and takes less time than ANN.
6) The results of feature extraction of a fingerprint image are supplied to CNN.
7) CNN may be used to do image segmentation, edge detection, fingerprint matching, and imagefeatures extraction.
8) 5*5 pixels are convolutionally filtered through a 3*3 pixel filter, resulting in 4*4 pixels.

VOTING

The voting page, which allows him or her to vote for any political party from a list of possibilities. They won't be able to change their mind after they've selected their chosen party, and the rest of the options will be disabled as well. Face detection and fingerprint matching are used to protect the voting system. The server accepts and saves the votes cast by verified voters. The number of votes cast for each political party's candidates will also be recorded. Even the counting of votes is simplified in this fashion, and the mission, candidates, and voters do not have to wait days for the results.

RESULTS

HTML is used to develop an internet website, and Visual Studio is used to implement the software scripts. The designed system outperforms existing technologies and is extremely safe. The CNN algorithm employed in the system makes it one-of-a-kind and efficient. It ensures that the voter's identity is verified before to the voting procedure. The Smart Voting System reduces and maybe eliminates the number of fraudulent votes cast, as well as making voting and countingof votes easier, more energy-efficient, accessible, and secure. Wrong votes can be reduced by using a secure network. The amount of manpower required can be minimized by using an online voting system.

Fig. 7. Website for voting where face recognition using live camera

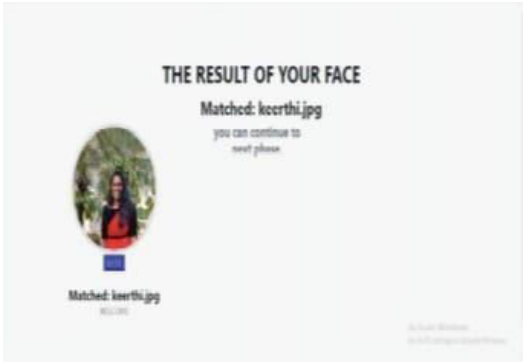


Fig.8. Result of face detection in real-time

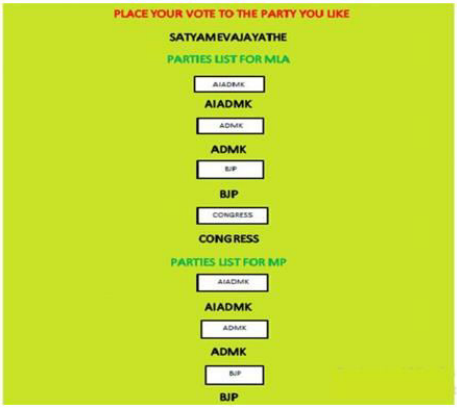


Fig. 9. The page where voting for preferred political party takes place

Fig.10. Face detection results

Fig.11. Mouth detection

Preprocessing results

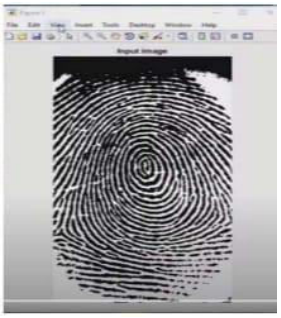


Fig.12. Input of Fingerprint image

Fig.13. Thinned image

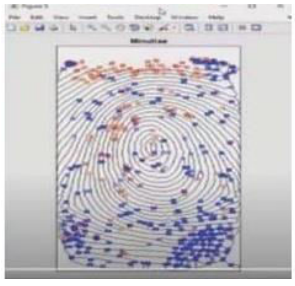


Fig. 14.Minutiae Results

Conclusion

The method that is more effective and secure than the current one is examined in this journal. There are fewer fraudulent votes than under the previous system, and voting takes less time. Age has no effect on distinctive characteristics like the distance between the brows and the eyes. Although fingerprint traits can be copied between two people, they cannot be changed. To find the database picture containing the voter fingerprint, we

can employ ten print images of minutiae records. Smart voting is also a better way to cast a ballot because the proposed system requires less time, money, and effort to operate.

REFERENCES

[1] Chandra Kirti Potina, Atla Indu Reddy, “Smart Voting Systems Using Facial Recognition,” IEEE Journal, April 2020.

[2] Anurag Chowdhury, Simon Kirchgasser, Andreas Uhl, Arun Ross "Does CNNs automatically learn the meaning of small dots to match fingerprints?" IEEE Conference, Mar 2020.

[3] Samarth Agarwal, Afreen Haider, “Biometrics Based Secured Remote Electronic Voting System”. IEEE Conference, Sep 2020.

[4] Suresh Kumar, Tamil Selvan G M, ”Block chain Based Secure Voting System Using Lot”, IEEE Journal, JAN 2020.

[5] Hanzhuo Tan, Ajay Kumar, "Towards Pose-Invariant Matching and More Accurate Contactless Fingerprint Minutiae Extraction" IEEE Conference 2020.

[6]. V. Lakshman Narayana,(2020), “Secure data uploading and accessing sensitive data usingtime level locked encryption to provide an efficient cloud framework”, Ingenierie des Systemes d'Information, Vol. 25, No. 4, 2020, pp- 515-519.

[7]. Pavani, Vellalachervu, and I. Ramesh Babu. "USING FOG AND REPLICATION TECHNIQUES INORDER TO ENHANCE CLOUD DATA SECURITY." Journal of Critical Reviews 7, no. 6 (2020): 202-207.

[8]. Sistla, Venkatramaphanikumar, et al. "Stacked Ensemble Classification Based Real- Time Driver Drowsiness Detection." Journal homepage: http://iieta. org/journals/ijsse 10.3(2020): 365-371.

[9]. Siva Koteswararao Chinnam, Sk.Reshmi Khadherbhi, P. Sandhya Krishna, D.Anveshini(2020), “Sentiment Analysis in Services Provided by Telecommunications”, International Journal of Advanced Science and Technology (IJAST)-Vol. 29, No. 03, pp. 9167 – 9176.

[10]. V. Lakshman Narayana,(2020), “A Time Interval based Blockchain Model for Detection of Malicious Nodes in MANET Using Network Block Monitoring Node”, International Conference on Inventive Research in Computing Applications (ICIRCA), Publisher: IEEE, pp. 852-857, 9183256.

[11]. K. Santhi Sri, Venkata Bhujanga Rao Madamanchi, D. Anveshini, V.Pavani (2020),“Secure Data Storage In The Cloud Using User Validation Method”, Journal of Critical Reviews(JCR)-Vol 7, Issue 6, pp. 391-395.

[13]. Medical data clustering using particle swarm optimization method, Lakshmi Patibandla, R.S.M., Tarakeswara Rao, B., Sandhya Krishna, P., Maddumala, V.R. Journal of Critical Reviews, 2020, 7(6), pp. 363–367

[14] Hui Xu, Miao Qi, “Multimode Biometrics Based on Convolutional Neural Networks UsingTwo-Layer Fusion” IEEE Conference, 2019

[15] Youssef El Merabet and Abdelleratif EI Idrissi, "State-of-the-art Local texture descriptors for Plam print Recognition."