DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4611

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

THE FRAMEWORK DESIGN FOR INCREASING SECURITY OF MULTI-MODAL BIOMETRIC AUTHENTICATION SYSTEM WITH DNN

Afshan Ashraf
M.Tech Student, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, Punjab, India.

Isha Vats
Assistant Professor, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, Punjab, India.

Abstract –This research paper defines a multi-modal system for verification based on the biometric fusion of retina, finger vein and finger print recognition. We have proposed feature extraction in retina recognition model by using SIFT and MINUTIA feature extract at work in different levels.Security is the main concept in ATM (Automated Teller Machines) today. Multi-modal Biometrics are secured as compared to uni-modal biometrics as even if single trait destroys the other is present. The application of multi-modal biometrics can be ATM. The proposed work, adds three biometric traits of a user namely retina, fingerprint and finger veins by an implemented software, later these are pre-processed and combined (Fused) together for score level fusion approach used. Retina is selected as a biometric trait as no binary retina feature matches unless they are of the similar user also retina has a good vessel pattern making it a good verifying approach as compared to other biometric traits. Security is found in the system by multi-modal biometric fusion of retina with finger vein and finger print. Feature Extraction approach and cryptography is used in-order to achieve security. The feature extraction is done with the help of MINUTIA and SIFT algorithm which are then classified using Deep Neural Network(DNN). The feature key points or minutiae points are fused at score level using distance average and later matched.The experimental result evaluated using MATLAB 2013a, illustrates the important enhancement in the performance of multi-modal biometric systems with higher values in GAR and FAR percentages.

Keywords—Biometric Fusion, Score Level Fusion, Minutiaes and Scale Invariant Feature Transformation, Deep Neural network

I. INTRODUCTION

The multi-modal biometric is a combination of two or more biometric traits. As evaluated to uni-modal biometrics multi-modal biometrics more reliable as various traits are used [1].

Various biometrics optimize the false acceptance rate and mean square error rate. It is more secure as it become complicated for an attacker to copy various biometric traits of a person; hence more security is attained to the system.

In real time example or application of multi-modal biometric can be in the security of ATM. The security is the major concept in ATM because PIN number could be easily hacked [2].

Biometrics can be considered as the quantity and analysis of biologic features of a user to consider his or her verification conclusively. It is not all physical biometric traits are acceptable for that matter. The major properties considered in case of the applications are acceptability, measurement, uniqueness etc. To obtain those properties, we consider two or more features of a single person to evaluate or confirm the ID of that single person[3].

The biometric fusion can be operated in four phases:

i. Sensor Level
ii. Feature Level
iii. Decision Level and
iv. Score Level [4]

Fusion at the scoring phase is normally used, as it gives the best trade-off between data richness and is easy to implement. To improve the performance in multi modal biometric fusion information and quality of information can prove to be of higher interest.

Most of the researchers have analyzed the quality management in case of score level fusion with combination of various traits such as retina, fingerprint and finger veins, Iris and fingerprint, facial and retina etc[9,10] .

In this proposed system, we work on multi-modal biometric traits i.e., retina, fingerprint and fingerveins. In retina and Vein recognition, we have implemented the scale invariant feature transform for feature extraction which gives us results in the form of key-points. In finger print recognition, we use minutia feature extraction algorithm to extract the unique features based on minutiae points. After that we apply the cryptography method to provide the security by using RSA algorithm [11].

We implement the score level fusion approach to provide security in the multi-modal biometric traits. Then, the fused features are saved in the database and classification approach to classify the features and performance evaluation is done using Deep Neural Network [12] .

II. RELATED WORK

"D. Jagadiswarya, D. Saraswady" [2016],[5] proposed Fused Multimodal systems which also have several advantages over uni-biometric systems such as, enhanced verification accuracy, larger feature space to accommodate more focuses and higher safety against spoofing. The proposed improved multimodal authentication system is based on feature extraction (using fingerprint, retina and finger vein) and key generation (using RSA).

"Amioy Kumar, Ajay Kumar"[2015],[6] used score level fusion technique to design a secure adaptive biometric fusion. They used two different biometrics i.e; hand and eye. Extracted features were passed through score level fusion process and optimization was done with ACO algorithm. The training set was used to store various processed features and test various input samples.

"R. Manjuand A. Shajinnargunam" [2016], [7] authors did a comparative study of various classifiers for secure authentication system called fusion. Authors did their research on three different biometric images. All the train and test samples were processed through salt and paper noise along with their filtration process. Filtered images processed through PCA algorithm for feature extraction process to minimize the input dataset with unique properties. Extracted features in this process passed through different classification techniques to form a comparative study on them.

"ShahendaSarhan, ShaabanAlhassan" [2016], [8] authors did a comparative study on different biometrics systems. In this study, the study on working of biometric systems is done on the basis of feature sets, training and testing of fused data. Authors worked with PCA algorithm for feature extraction and dataset generation. All the performance parameters are calculated on the basis of score level fusion and matching results of input samples to the dataset used by author in this research. Performance of various biometric databases is calculated through the detection accuracy of proposed approach in this research. Fingerprints show maximum accuracy in the overall results as 94.70% in this research.

III. SYSTEM BLOCK DIAGRAM

Step 1: Search a multi-modal biometric (Retina, Fingerprint and Finger Veins) data set form the UCI MACHINE REPOSITORY site and download it. Upload the Retina, Fingerprint and Finger Vein recognition image from the database. Convert the original image to gray-scale image to reduce the original image pixel size. Identify the noise level in the gray-scale image and reduce the attack or noise in the image. Detect the RGB component (Red, Green and Blue) to gray scale conversion.

Step 2: After this, we implement the edge detection approach to calculate the edges in particular biometric model. Canny edge detector is also known as optimal edge detector, in which edges describe boundaries. Edge detection is of vital significance in image processing. Edges describe the area with robust intensity and contrast that is a jump in intensity from one pixel to another pixel. Edges detect the image significantly and filter out the useless information and reduces the amount of data.

Step 3: In this step, we implement the scale invariant feature transform in case of retina and finger veins and Minutiae feature extraction algorithm in case of fingerprints to extract the particular features from various biometric traits. The features are extracted in case of SIFT algorithm in the form of key-points. Minutia algorithm generates three images i.e, binary image, thin image and minutiae features represented in red and blue form.

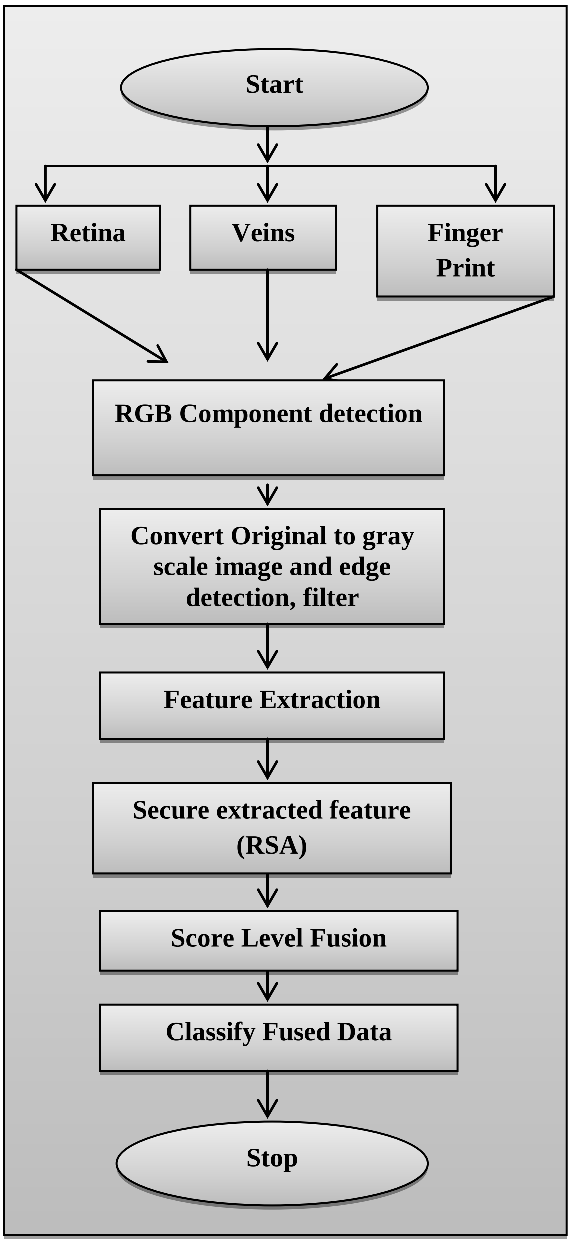


Fig 1. Proposed Work

Step 4: We implement the score level fusion which is the fusion of the three biometric traits for authentication system. Each feature in the database is same as the fused data and and can be represented graphically.

Step 5: We implement the RSA algorithm for encrypting the information with the help of two prime numbers used. First, the public data is visible to every person but private data is not visible to any other person and a secret key is used to convert the public data into private data.

Step 6: In this step, we implement the classification algorithm i.e; deep neural network. This algorithm consists of an input and output layer in between which there is a hidden layer where all the data is classified and filtered and then passed to the output layer. This algorithm is used to classify the biometric authentication system and evaluate the performance parameters i.e (FAR, FRR, GAR and Accuracy).

Step 7: Compare the performance parameters with the existing performance parameters i.e (FAR – False Acceptance rate and GAR- Genuine Acceptance Rate).

IV. Result Explanation

This section determines the evaluated results of the proposed digital image processing concept for Biometric traits i.e; Retina, Finger Print and Finger Veins. The proposed image processing concept is implemented in MATLAB with GUI (Graphical User Interface).

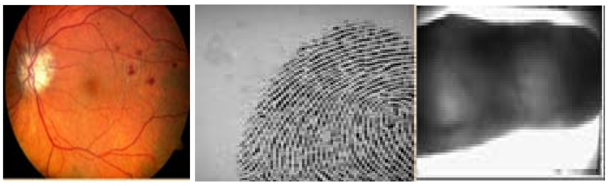


Fig 2.Original Image (Retina, Finger print and Vein)

Figure 2 shows the Upload of the original image in case of retina, Finger Print and Finger veins.

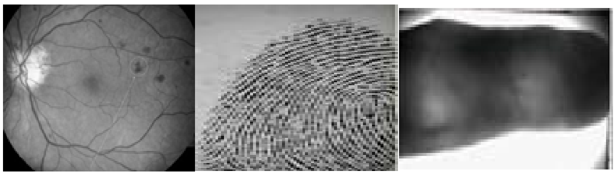


Fig 3. Gray Scale Image

The above figure3, represents the conversion of original image to gray scale image to reduce the original image pixel in case of retina, finger print and veins.

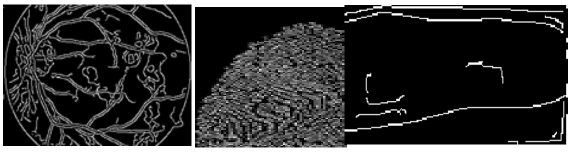
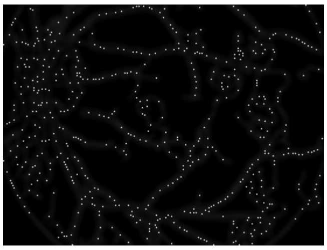
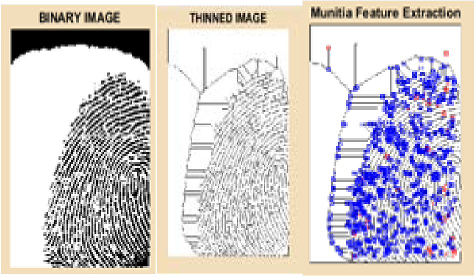


Fig 4. Edge Detection (Canny and Sobel)

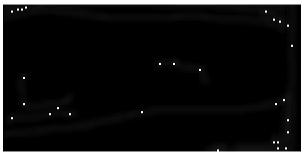
The above figure 4 shows the edge detection technique using Canny property. In this property, the edges detect the maximum, minimum and average value of the gray scale image.Edge detection using Sobel technique is the detection of one at a time each value i.e; minimum, maximum and average value.



(i)



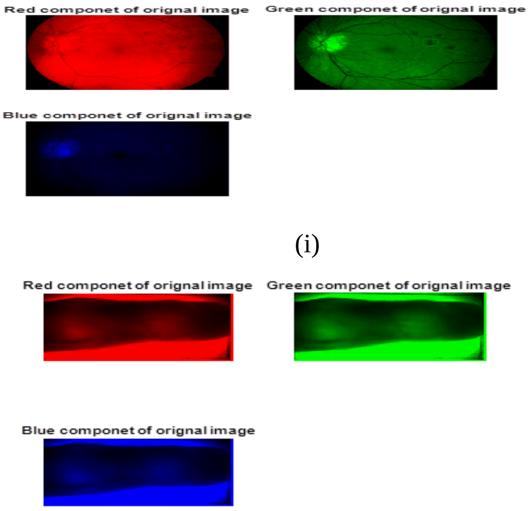
(ii) (iii) (iv)



(v)

Fig 5. Feature Extraction

The above figure 5 shows the feature extraction by applying the Scale Invariant Feature Transform in retina image which extracts the Key point values and are represented in matrix form. The features are extracted in case of fingerprint images with the help of minutia feature extraction algorithm. This technique found the features in three steps i.e; extraction of the binary image, thinned image and Minutia feature extract in the colour representation i.e read and blue.



Red componet of orignal image
Green componet of orignal image
Blue componet of orignal image
Red componet of orignal image
Green componet of orignal image
Blue componet of orignal image

(i)

(ii)

Fig 6 RGB component detection

The figure represents the red, green and blue component analysis in 3D form.

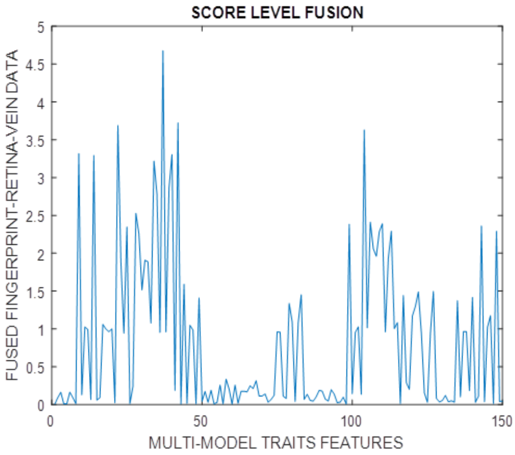
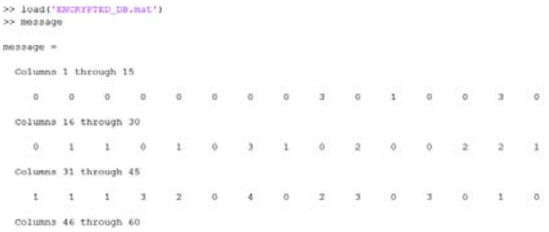


Fig 7. Score Level Fusion

The above figure 7 shows the score level fusion used for fusion in case of multi-modal biometric system means using high security, merging three biometric traits and then fusing the three traits only if dataset equality is same.



```
>> load('ENCRYPTED_DB.mat')
>> message

message =

  Columns 1 through 15

     0     0     0     0     0     0     0     0     3     0     1     0     0     3     0

  Columns 16 through 30

     0     1     1     0     1     0     3     1     0     2     0     0     2     2     1

  Columns 31 through 45

     1     1     1     3     2     0     4     0     2     3     0     3     0     1     0

  Columns 46 through 60
```

Fig 8. Encrypted data

The above figure represents the encrypted data by using RSA algorithm taken out with the help of two prime numbers. The secret key is used to convert the data into private information and then to public information again.

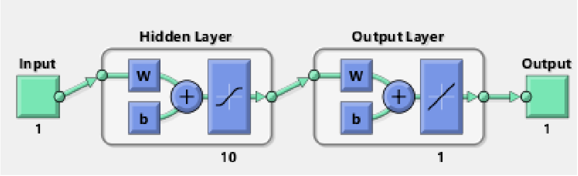
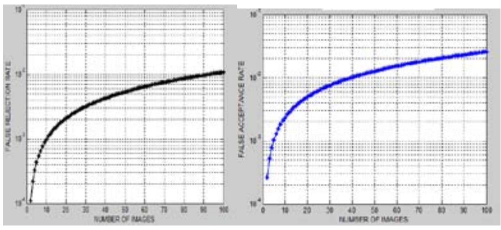
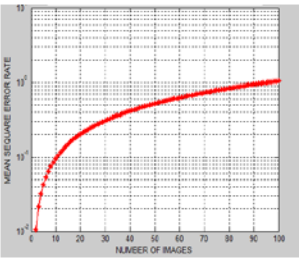


Fig 9. Deep Neural Network

The above figure represents the classification approach using deep neural network. It generates the values in the form of keypoints. If the values obtained are the same as the values obtained from score level fusion done in testing phase, then the system shows a perfect match otherwise the system shows a mixed match.



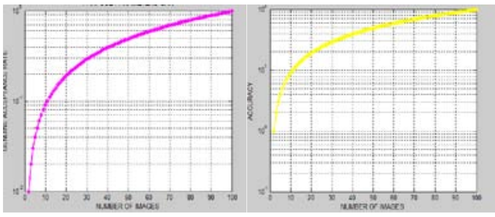
(i) (ii)



(iii)

Fig 10 False rejection and Acceptance Rate , Mean Square Error Rate

The above figure 10(i) and (ii) shows the false rejection rate which is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.The above figure 10 (iii) defines MSE which is a frequently used measure of the differences between values (sample and population values) predicted by a model or an estimator and the values actually observed.



(i) (ii)

Fig 11. Genuine Acceptance rate and Accuracy rate

The figure 11(i) and (ii) defined the Genuine Acceptance Rate based on the true values. This is defined as a percentage of genuine users accepted by the system.The above figure represents accuracy of a test and its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases.

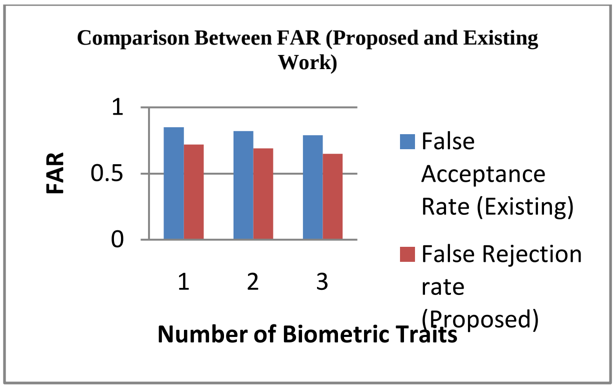


Fig 12. Comparison BetweenFAR proposed and Existing Work (Bar Graph)

Above figure shows that the false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

Table no.1 Comparison Between False Acceptance Rate(Base and Proposed Work)

Biometric Traits	FAR(Existing)	FAR(Proposed)
Fingerprint, Retina and Vein	0.85	0.72
Retina , Vein and Fingerprint	0.82	0.69
Vein , Fingerprint and Retina	0.79	0.65
Fingerprint, Retina and Vein	0.85	0.72

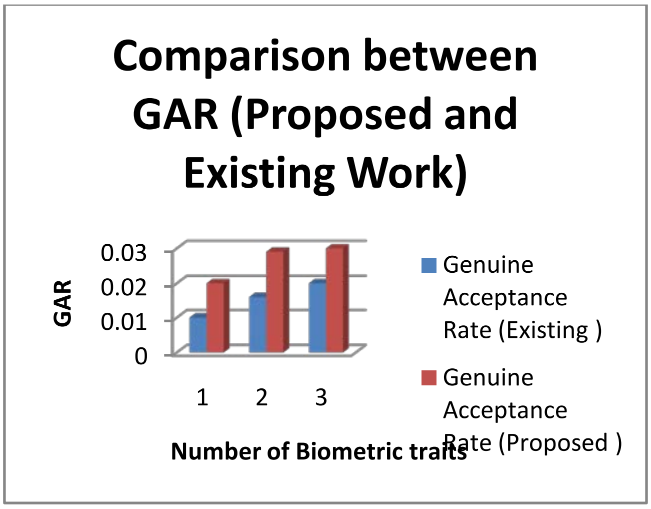


Fig 13. Comparison Between GAR(Existing and Proposed Work)

Table no.2 Comparison Between Genuine Acceptance Rate(proposed and existing)

Biometric Traits	GAR(Existing)	GAR(Proposed)
Fingerprint, Retina and Vein	0.01	0.02
Retina , Vein and Fingerprint	0.016	0.029
Vein , Fingerprint and Retina	0.02	0.03
Fingerprint, Retina and Vein	0.01	0.02

V. Conclusion and Future Scope

The score level fusion technique is used for the design of multimodal biometric traits such as fingerprint, retina and finger vein, which protects the multiple templates using RSA and DNN. It has been implemented using MATLAB R2013a. A realistic security analysis of the multimodal biometric cryptosystem has also been conducted using fingerprint, finger-vein and retina, which provide a remarkable improved performance in a multimodal biometric cryptosystem using RSA and DNN classification approach. This thesis has proposed verification system based on retina, fingerprint and finger vein recognition. In the proposed system a new technique is generated at score level fusion to increase the performance of the retina, fingerprint and finger veins recognition authentication system. In this multimodal system, feature extraction is done using SIFT algorithm, RSA is used for encryption and DNN is used classification.

The overall performance of multimodal system has increased with GAR by 98.9%, Accuracy value is 98.5% and reduced with FAR of 0.05%, which as compared to uni-modal biometric systems is very high.

Future work can be further extended by accurately modelling feature extraction techniques and using wavelet transformation approach and managing the database more effectively and evaluating the matching methodology and its performance of biometric system using different level of fusion with Fuzzy Interference system.

VI. REFERENCES

[1] Dandawate, Yogesh H., and Sajeeda R. Inamdar. "Fusion based Multimodal Biometric cryptosystem." In Industrial Instrumentation and Control (ICIC), 2015 International Conference on, pp. 1484-1489. IEEE, 2015.

[2] Kihal, Nassima, SalimChitroub, and Jean Meunier. "Fusion of iris and palmprint for multimodal biometric authentication."In Image Processing Theory, Tools and Applications (IPTA), 2014 4th International Conference on, pp. 1-6.IEEE, 2014.

[3] Khiari-Hili, Nefissa, Christophe Montagne, Sylvie Lelandais, and KamelHamrouni. "Quality dependent multimodal fusion of face and iris biometrics."In Image Processing Theory Tools and Applications (IPTA), 2016 6th International Conference on, pp. 1-6.IEEE, 2016.

[4] Connaughton, Ryan, Kevin W. Bowyer, and Patrick J. Flynn. "Fusion of face and iris biometrics."In Handbook of Iris Recognition, pp. 219-237. Springer London, 2013.

[5] Jagadiswary, D., and D. Saraswady. "Biometric Authentication Using Fused Multimodal Biometric." Procedia Computer Science 85 (2016): 109-116.

[6] Kumar, Amioy, and Ajay Kumar. "Adaptive management of multimodal biometrics fusion using ant colony optimization." Information Fusion 32 (2016): 49-63.

[7] Manju, R. "Estimation of performance in multimodal biometric based authentication system using various clustering." Indian Journal of Science and Technology 9, no. 13 (2016).

[8] Sarhan, Shahenda, ShaabanAlhassan, and Samir Elmougy. "Multimodal Biometric Systems: A Comparative Study." Arabian Journal for Science and Engineering 42, no. 2 (2017): 443-457.

[9] L. Hong, Y. Wan, A.K. Jain. Fingerprint image enhancement algorithm and performance evaluation. In IEEE Transactions on Pattern Analysis and Machine Intelligence 20(8), pages 777-789, 1998.

[10] L. Hong, Y. Wan, A.K. Jain. Fingerprint image enhancement algorithm and performance evaluation. In IEEE Transactions on Pattern Analysis and Machine Intelligence 20(8), pages 777-789, 1998.

[11] Bicego, Manuele, Andrea Lagorio, Enrico Grosso, and Massimo Tistarelli. "On the use of SIFT features for face authentication." In Computer Vision and Pattern Recognition Workshop, 2006.CVPRW'06. Conference on, pp. 35-35. IEEE, 2006.

[12] Bicego, Manuele, Andrea Lagorio, Enrico Grosso, and Massimo Tistarelli. "On the use of SIFT features for face authentication." In Computer Vision and Pattern Recognition Workshop, 2006.CVPRW'06. Conference on, pp. 35-35. IEEE, 2006.