International Journal of Computer Networks and Communications Security

VOL. 5, NO. 9, SEPTEMBER 2017, 198–204
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Liveness Authentication of Iris Template: A Data Mining Approach

Maqsood Mahmud

Department of Managment Information Systems (MIS), College of Business Adminsitration (CBA), Imam Abdulrahman Bin Faisal (IAF) University, Dammam, Kingdom of Saudi Arabia

mmahmud@uod.edu.sa

ABSTRACT

The liveness authentication is very important in the surveillance environment, especially in border crossings and places where there is a buffer zone or war area. In this paper, it is determined how to test the liveness of the iris template to avoid fraud. Various data mining can be used to achieve this phenomenon. There are basically two methods for liveness authentication i.e. static and dynamic. A method is proposed in this paper based on the combination of static and dynamic methods. A data mining tool is used to generate graphical results based on combination of classification and clustering algorithms. Twenty features were defined to authenticate the liveness authentication. The visual results are presented to validate the results. It was found that J48 is the best classification algorithm for determining the liveness detection rather than DBSCAN. It is concluded that liveliness of iris can be determined by using the soft biometrics.

Keywords: *Biometrics, Iris Liveness Detection, Classification, Clustering, Data mining, WEKA*.

1 INTRODUCTION

Liveness authentication is an important aspect of true authentication. In the proposed model, various aspects are taken into account. Sensing air blown from the mouth during authentication process is considered. Implementation of the Gaussian Filter on the acquired image to check the level of noise in the image is considered. If abnormal noise is detected, then liveness authentication may be rejected as one factor in the model. Fourier's plan to deal with colour contact lens are also applied to validate liveness. Temperature of the face/iris is another parameter brought into consideration. Abnormal eye movement due to gelatine lens or plastic cover on eye or glass lenses may also give a clue for the liveness detection [1-3].

Iris Biometric Template Security is carried by most of researchers [3] highlighted that iris template security is a main problem that should be tackled. This is required when biometric authentication system designing is processed. The essential requirement during the design of biometric based system is template protection. For these methods, it is assured that stored template cannot be accessed by illegal users. User information can be revealed from a template. Identity theft is another issue that may arise during iris biometric authentication. To consider this issue, it seems to be of high importance when an iris template is hacked. Template distortion techniques are used to protect the template. The biometric cryptosystems and data hiding techniques can also be used. A template may be kept secret because of two reasons i.e. privacy and security. If an iris template is hacked, it should be essential to rescind it or cancel it or replenish it for security and privacy reasons. Moreover, it is also preferable to get various templates from one biometric so illegal users can be thwarted across various databases. It is suggested to glean from the similar biometric data with dissimilar data templates so that one can get rid of unlawful accessing across dissimilar data wares. Recently various methods have been presented to protect biometric template and give a favourable celability phenomenon and renewability characteristic to the biometric systems. Moreover, newly introduced methods i.e., template deformation, biometric encryption of templates, and data hiding methods are of significance according to current research.

Active areas of research are the techniques for match on card, liveness detection, system on chip, and template fortification techniques. Template protection techniques specially pinpoint essential security issues. These include how hacked

templates can be recovered. In case an intruder gets access to biometric methods, it is important to have a recovery technique to prevent intruders to repeat. Breaching multiple systems is often simultaneously difficult for the intruders. Considerable progress is required in the area and especially in the model of template defence technique. It provides good security along with identification correctness. Matching on card, system on device and system on a chip system produce awareness due to its support for a decentralized operation. In this way users achieve security from biometric data templates which were mostly in control of an anti-tamper device. Smart cards are used for most of the credentialing programs for storage of biometric templates. The feature extraction and matching also is presently executed exterior of the tag or card [3-5].

In [8-9] Jain and Lee proposed a scheme for securing biometric templates of variable sizes. The proposed technique is composed of a new similarity measure approach. It is named 'the set intersection'. It vigorously matches the methodologies used in the state of the art biometric matching prototype. The proposed scheme is tested in consideration of security and performance.

In [10-13] authors elaborated that dissimilarity in the control range of parts from regularized biometric iris data images is the extraction for coding a human iris. They applied their technique on 2174 images from 308 eyes. Results of 100% right identification were obtained utilizing a prejudiced Hamming Distance parameter for recognition purposes. A verge is defined for the distance metric and false reception and false refusal rates. It is also recorded. These techniques achieved the minimal fake reception rate at the point of first fake refusal. This comparison was made surrounded by the three methods verified, with the least complication of the algorithm.

In [4] Daugman described that the similarity metrics are the key techniques used in mostly biometric recognition systems. These metrics allow decisions of "same" or "different" templates. Making these templates compatible for matching these metrics has to pass through normalization gates. The probability of high-quality match increases by probability between distinct templates which has to augment with the volume of the dataset. For iris recognition in publicly deployed sites, biometric similarity score normalization plays a vital role in False Matches which are to be avoided.

According to [6-7] the author sketched back-ground of the iris template liveness detection techniques. It further elaborates that the iris is a physical muscle inside the human eye ball, controlling the dimensions of the pupil. In this way it directs the quantity of sun or bulb beam that cross the threshold of the human eye. The iris is the pigmented element of the human eye. Iris identification utilizes the arbitrary, pigment ranges inside the iris. These colour ranges are exclusive to every human being. Liveness verification is precise for a scrupulous biometric modality. It is approximately divided in two groups. Static verification calculates a number of physical features, which can be fingers or facial warmth. It distinguishes between the live human being and a synthetic fake body. Dynamic verification confirms the response of an individual to action or impulse. This action might be augmented in beam strength to observe the pupil retrenchment. It can be requesting an individual to articulate a particular specific expression or sentence. Research is being carried out in this area. Various people are articulating their own work for static and dynamic verification.

Iris recognition as a trustworthy technique for personal identification has been thoroughly studied with the aim to allocate the class label of each iris image to a distinct subject. Contrary, iris image classification aims to categorize an iris image to an application particular category, e.g., iris liveness detection i.e. classification of real and forged iris images, race classification e.g., classification of iris images of Asian and non-Asian subjects, coarse-to-fine iris recognition i.e. categorization of all iris images in the central database into multiple categories [17]. Smartphone's have been extensively used with a vast array of susceptible and personal information stored on these devices. To protect such information from being leaked, user authentication schemes are necessary. Existing password/pattern-based user authentication mechanism is susceptible to shoulder surfing attacks and blotch attacks [25].

2 METHODOLOGY

The following framework is proposed for effective methodology. The dataset chosen is world's most popular IRIS Dataset i.e. CASIA dataset for IRIS. One can use dataset of ATVS, LivDet2009, and LivDet2011 etc. The attributes are selected for the said dataset to authenticate the liveness. In this method, 20 attributes will be carefully selected for experimentation. These features are the combination of static and dynamic features for liveness detection. Static verification calculates a number of physical features can be fingers or facial warmth. It distinguishes between

the live human being and a synthetic fake body. Dynamic verification confirms the response of an individual to action or impulse. This action might be augmented in beam strength to observe pupil retrenchment. It can be requesting an individual to articulate a particular specific expression or sentence [14-20]. So, in the proposed methodology 20 mixed features are selected from both static and dynamic verification method of liveness as shown in Figure 2.1. Some of the examples are (i) person's body motion, (ii) mouth air blow, (iii) saccade, vein pulse, (iv) detection of hippus, (v) person's "ID", (vi) Gaussian filter effect, (vii) person's head movement, (viii) focussing of eye, (ix) normal occlusion, (x) person's age, (xi) name of person on hit list, (xii) abnormal external colour of ear, (xiii) focussing of eye, (xiv) determination of sex of person whether male or female, (xv) abnormal Fourier transform value of iris image and comparing with live image, (xvi) normal eye tears in comparison with abnormal eye tears by some impulse (e.g. tear gas etc), (xvii) abnormal face/iris temperature, (xviii) abnormal external nostril, (xix) head movement and (xx) abnormal body vibration.

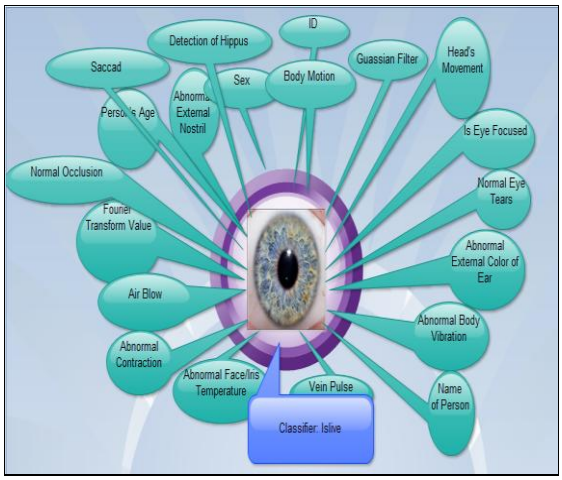

Fig. 2.1. Proposed Multi-Factor Liveness Authentication Model (MLAM)

Figure 2.2 is a WEKA file consisting of three portions. It depicts all the 20 features/attributes discussed above. The file below starts with "@" followed by relation name e.g. "livedetec". The second portion specifies attribute name and type. It begins with the keyword "@" followed by a keyword "attribute" then the attribute name and its type. The third portion of the file consists of data. It begins with keyword "@data" and the then all data values are mentioned according to attributes mentioned above separated by a comma.

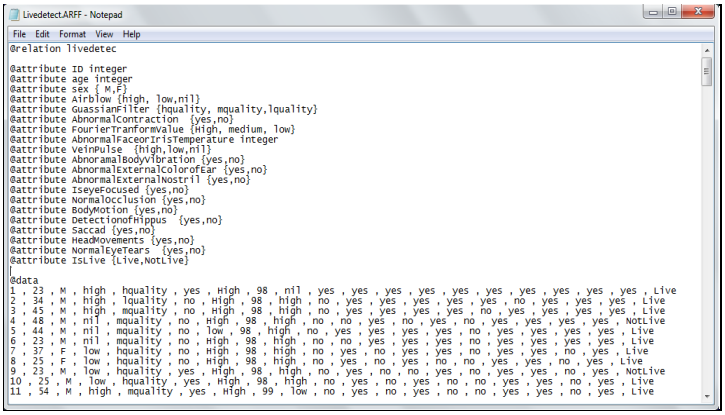

Fig. 2.2. Liveness Detection Features in WEKA (ARFF File)

3 RESULTS AND DISCUSSION

The following results are achieved by using the classification and clustering algorithms. The results are discussed in detailed in Section 3.1 and 3.2, respectively.

3.1 Liveness Detection Using J48 Classification Tree Algorithm

Results in the following paragraphs show the liveness detection using J48 classification tree algorithm. Table 3.1 shows a confusion matrix for J48. There are two classifiers in the matrix i.e. (i) A=Live and (ii) B=NotLive. The table shows the number of Live classified as 199 and notLive classified as 16. The two classifiers are the "Live" and "NotLive".

Table 3.1: Confusion Matrix for J48

Actual Class	**Predicated**	
A=Live	199	13
B=NotLive	16	122

The Table 3.2 shows three matrices i.e. number of J48 tree leaves, size of J48 tree and the time (seconds) taken to build the model. The number of leaves found to be 10, size of J48 tree is 17 and the time taken is 0.14 seconds.

Table 3.2: J48 Tree Details

Metrics	**Quantity**
Number of Leaves	10
Size of Tree	17
Time Taken to build model	0.14 Seconds

Table 3.3 shows the stratified cross validation summary. In this table correctly classified instances, incorrectly classified instances, kappa statistics, mean absolute error, root mean square error, relative absolute error, root relative squared, and total number of instances are shown categorically.

Table 3.3: Stratified cross-validation Summary

Metrics	Number Value	Percent Value
Correctly Classified Instances	321	91.7143%
Incorrectly Classified Instances	29	8.2857%
Kappa Statistics	0.8259	Nil
Mean absolute error	0.136	Nil
Root mean squared error	0.2781	Nil
Relative absolute error	Nil	28.467%
Root relative squared	Nil	56.9014%
Total Number of Instances	350	Nil

Figure 3.1 represents J48 classification tree based on the 20 features proposed in the paper. The overall classification is based on the live and not live classification. J48 tree helps to determine the liveness of the iris template. The tree on every branch tries to determine the liveness of iris from top to bottom. Accuracy of the results may be achieved at any level of tree depending upon the proper features selection and optimization techniques of attributes.

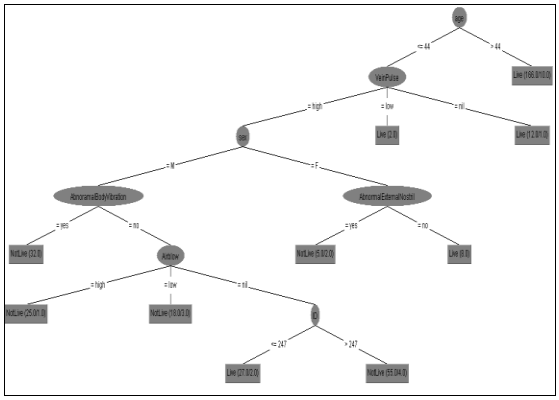

Fig. 3.1. Classification J48 Tree Algorithm on the data

Table 3.4 is the detailed result of J48 according to true positive (TP), false positive (FP), precision, recall values, F-measure, ROC area and at the end class (Live, NotLive). The TP gives the measure of true positive which is 0.939 for live, 0.884 for not live and 0.917 for an average case. Similarly the FP rate is determined as 0.116 for live, 0.904 for NotLive, 0.917 for average case. Precision values comes to be 0.926 for live case, 0.904 for not live and 0.917 for average cases. Recall is 0.939, 0.884, 0.917 for Live, not live and average case respectively. F-Measure is for live is 0.932 and not live is 0.894 while the average case it is 0.917. The ROC area of live, notLive and Average case are same, which is 0.893 value.

Table 3.4: Detailed Results of J48

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
0.939	0.116	0.926	0.939	0.932	0.893	Live
0.884	0.061	0.904	0.884	0.894	0.893	Not Live
0.917	0.094	0.917	0.917	0.917	0.893	Weighted Avg.

Figure 3.2 shows the J48 classifier errors. Errors are shown in blue and red colours for Live and NotLive cases. Blue colour represents Live classifier errors while red colour represents NotLive errors. The upper portion of NotLive is more populated/congested with Live and NotLive classification errors showing the maximum error area. The mid and bottom portion of Figure 3.2 on right corner of Figure 3.2 are minimal with respect to classification errors.

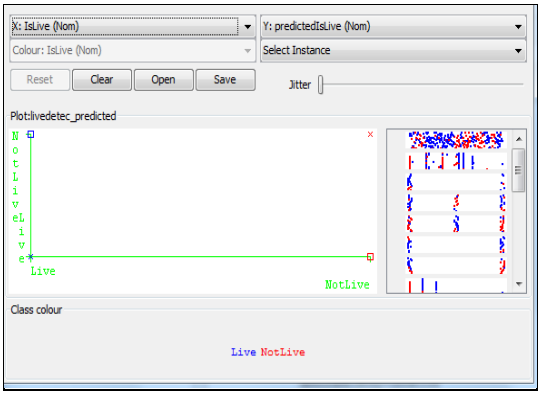

Fig. 3.2. Visualizing J48 Classifier errors

3.2 Attribute Using Clustering DBSCAN

The results show the implication of DBSCAN algorithm on the proposed liveness authentication model. Table 3.5 represents the results achieved with DBSCAN algorithm which is unsupervised classification. The table shows metrics and quantity. The quantity clustered data objects are found to be 350, number of attributes were 20, Epsilon is 0.9, Min points are 6, number of generated clusters are 10, Elapsed time of the clustering classification was found to be 0.57 seconds. The time taken to build model i.e. full training data was also 0.57. These results are from DBSCAN which is unsupervised classification.

Table 3.5: DBSCAN Results (Unsupervised Classification)

Metrics	Quantity
Clustered Data Objects	350
Number of attributes	20
Epsilon	0.9
Min Points	6
Number of generated clusters	10
Elapsed time	0.57
Time taken to build model (full training data) in seconds	0.57

Table 3.6 shows model and evaluation on the training set. The clustered instances are shown for 10 different percent values. The unclustered instances are 48 in the training set. The highest value is on cluster "3" which is 108 (36%) while the lowest value is for cluster "4" which is 6(2%). Total instances are 100 out of which 48 instances are remained unclustered which are specified as above in the beginning.

Table 3.6: Model and Evaluation on Training Set

NO.	Clustered Instances
0	10 (3%)
1	13 (4%)
2	23 (8%)
3	108 (36%)
4	6 (2%)
5	30 (10%)
6	14 (5%)
7	27 (9%)
8	22(7%)
9	49 (16 %)
Unclustered Instances	48

Figure 3.3 shows the clustering assignment graph based on DBSCAN algorithm which is unsupervised classification. Figure 3.3 shows a total of 10 clustered plot with different colours. A strait bar is formed with the DBSCAN algorithm to depict formation of clustered based on 20 attributes selected for live and notLive detection. Although unsupervised classification proved to be less helpful in the determination of live and notLive determination of iris templates, it still gives some clues about the liveness detection.

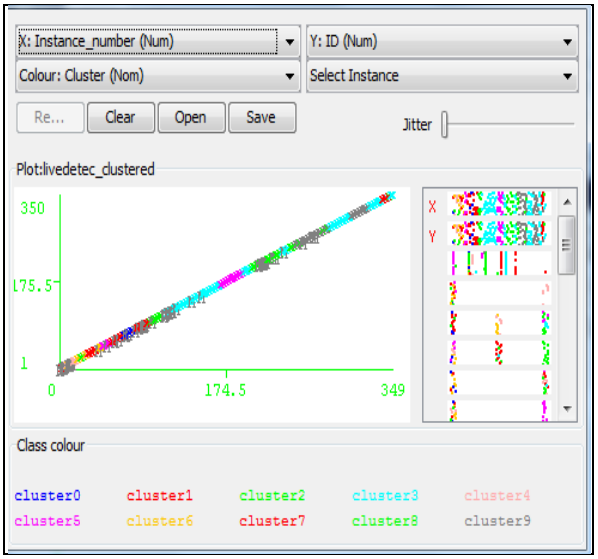

Fig. 3.3. DBSCAN Clustering Assignments graph

3.3 Selected Attribute for performance using BestFirst Method

The following results show the best first method for liveness authentication model in the dataset given. Figure 3.4 shows graph of reduced data. This reduced data graph is achieved by selecting specific attributes among twenty proposed attributes. The BestFirst method helps in reducing the attributes which is more beneficial in optimization of the Live and NotLive cases. This way performance is enhanced. Although BestFirst method carries less importance to proposed attributes because of a lesser number of attributes. The importance of the BestFirst method is realized when thousands of attributes are involved in determining a class. So, the BestFirst needs to be used in large set of attributes to give best results.

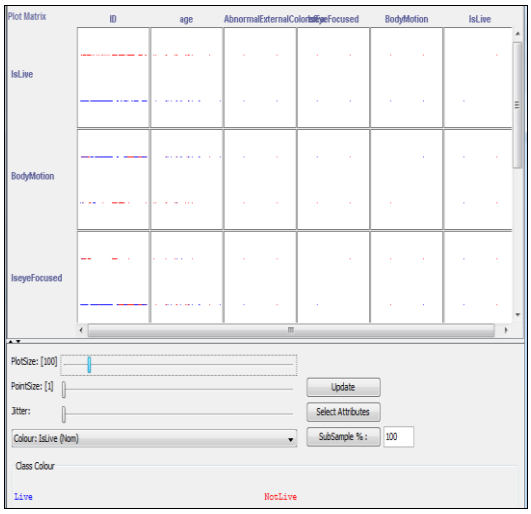

Fig. 3.4. Graph of reduced data

4 CONCLUSION

The fake liveness techniques can be used by illegal immigrants, organizational thieves, and suicidal attackers when they succeed to enter in the secure zone and in human traffic controlling areas. The model proposed in the paper covers various aspects so that liveness authentication will succeed and security cannot be compromised at any cost. The J48 tree which is supervised algorithm is proved to be more deterministic for liveness detection in respect to DBSCAN which is unsupervised classification.

5 LIMITATION AND FUTURE WORK

More advance classification algorithms can be applied to validate the liveness along with various features. These limitations and future directions open gates to other researchers working in the same field of iris code biometric template security and liveness authentication of biometric data.

6 ACKNOWLEDGEMENT

This work was supported by College of Business Administration (CBA), Deanship of Scientific Research (DSR), Imam Abdulrahman Bin Faisal University (IAF), Dammam, Saudi Arabia under research project number 2017-248-CBA. The authors are grateful for this support.

6 REFERENCES

[1] Alraisi, and Alkhouri, Iris recognition and the challenge of homeland and border control security in UAE. Journal of Telematics and Informatics, 25(2), 117–132, (2008).

[2] Boatwright, M., and Luo, X. What Do We Know About Biometrics Authentication?. Proceedings of the 4th annual conference on Information security curriculum development (InfoSecCD). (2007) 28 - 29 September. New York, NY, USA

[3] Bowyer, K. W.,Hollingworth, K., Flynn, P. J. Image Understanding for Iris Biometrics: A survey. Computer Vision and Image Understanding Elsevier.110(2), 281–307(2008).

[4] Daugman J. High Confidence Visual Recognition of Persons by a Test of Statistical Independence. IEEE Transaction on Pattern Analaysis Machine Intelligence (PAMI), 15(11),1148-1161(1993).

[5] Deluisgarcia, R., Alberolalopez, C., Aghzout, O., and Ruizalzola, J. Biometric identification systems. Signal Processing, 83(12), 2539–2557 (2003).

[6] El-Sisi A, Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter, The International Arab Journal of Information Technology, 8(4), pp 355-363 (2011).

[7] Galbally, J. Ortiz L. J, Fierrez, J. and Garcia, J. Iris Liveness Detection Based on Quality Related Features. 5th IAPR International Conference on Biometrics (ICB), (2012) 29-31 March. New Delhi, India

[8] Jain, A. Hong, L. and Pankanthi, S. Biometric Identification. Communications of the ACM. 43(2), 91-98. (2000).

[9] Jain, A. K., Nandakumar, K., and Nagar, A. Biometric Template Security. EURASIP Journal on Advances in Signal Processing, 8(1), 1-18. (2008).

[10] Kim, W. Towards real biometrics : An overview of fingerprint liveness detection. Annual Summit and Conference on Signal and Information Processing Association (APSIPA), (2017) 13-16 December 2106, Asia-Pacific

[11] Lee, E. C., and Park, K. R. Fake iris detection based on 3D structure of iris pattern. International Journal of Imaging Systems and Technology, 20(2), 162–166 (2010).

[12] Mahmud,M., Khan,M., Alghathbar, K., Abdullah,A. and Idris, M.B., Intrinsic Authentication of Multimedia ObjectsUsing

Biometric Data Manipulation, The International Arab Journal of Information Technology, 9(4), 336-342 (2012).
[13] Poursaberi, A., and Araabi, B. N. Iris Recognition for Partially Occluded Images: Methodology and Sensitivity Analysis. EURASIP Journal on Advances in Signal Processing, 7(1), 1–13. (2007).
[14] Prabhakar, S. Biometric Recognition: Security And Privacy Concerns. IEEE Security , 4677(2), 275–42 (2003).
[15] Rejman-greene, M.. Secure Authentication Using Biometric Methods. Information Security Technical Report, 7(3), 30–40 (2002).
[16] Roberts, C. Biometric Attack Vectors And Defences. Computers and Security, 26(1), 14–25. (2007).
[17] Sun, Z. and Zhang, H. Iris Image Classification Based on Hierarchical Visual Codebook, IEEE Transactions on Pattern Analysis and Machine Intelligence 36(6), 1120 - 1133 (2014).
[18] Vetro A., Draper S, Rane S, Yedidia J. Securing Biometric Data. Distributed Source Coding, USA: Academic Press, Mitsubishi Electric Research Laboratories. 45, 1-16 (2009).
[19] Shannon E.C. A Mathematical Theory of Communication, The Bell System Technical Journal,27(1), 379–423 (1948).
[20] Tamura, Y., and Tanaka, T. Personal Authentication By Analysis Of Iris, Annual Conference SICE. 4-6 August. Sapporo, Japan, 239–242 (2004).
[21] Venugopalan, S. , Savvides, M. How to Generate Spoofed Irises From an Iris Code Template, IEEE Transactions on Information Forensics and Security. 6(2), 385-395 (2011).
[22] Vrcek, G., and Peer, P. Iris-Based Human Verification System: A Research Prototype. 16th International Conference on Systems, Signals and Image Processing. (2009) 18-20 June. Chalkida, Greece
[23] Wu, X., Wang, K., Zhang, D., and Qi, N. Combining Left and Right Irises for Personal Authentication, 6th International Conference, EMMCVPR. (2007) 27-29 August. Ezhou, China
[24] Zhou, X, Busch and Christoph. Measuring privacy and security of iris fuzzy commitment, IEEE International Carnahan Conference on Security Technology (ICCST), (2012) 15-18 Octobar. Newton, MA, USA
[25] Zhu, H., Hu, J. and Chang, S., ShakeIn: Secure User Authentication of Smartphones with Habitual Single-handed Shakes IEEE Transactions on Mobile Computing. 99, 1-1.