ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Disposable Feature Templates Using Biometric Systems

C. Sujatha[1], K.Sridar[2]

PG Scholar, Veerammal Engineering College, K. Singarakottai, Tamil Nadu, India[1]

Assistant Professor, Department of CSE, Veerammal Engineering College, K. Singarakottai, Tamil Nadu, India[2]

ABSTRACT: Biometric access control systems are becoming more commonplace in society. However, these systems are susceptible to replay attacks. During a replay attack, an attacker can capture packets of data that represents an individual's biometric. The attacker can then replay the data and gain unauthorized access into the system. Traditional password based systems have the ability to use a one-time password scheme. This allows for a unique password to authenticate an individual and it is then disposed. Any captured password will not be effective. Traditional biometric systems use a single feature extraction method to represent an individual, making captured data harder to change than a password. There are hashing techniques that can be used to transmute biometric data into a unique form, but techniques like this require some external dongle to work successfully. The proposed technique in this work can uniquely represent individuals with each access attempt. The amount of unique representations will be further increased by a genetic feature selection technique that uses a unique subset of biometric features. The features extracted are from an improved genetic-based extraction technique that performed well on periocular images. The results in this manuscript show that the improved extraction technique coupled with the feature selection technique has an improved identification performance compared with the traditional genetic based extraction approach. The features are also shown to be unique enough to determine a replay attack is occurring, compared with a more traditional feature extraction technique.

KEYWORDS: Evolutionary Computation; Cyber Security; Periocular Recognition; Biometrics; Feature Selection

I. INTRODUCTION

Biometrics human characteristics and traits can successfully allow people identification and authentication and have been widely used for access control, surveillance, and also in national and global security systems. In the last few years, due to the recent technological improvements for data acquisition, storage and processing, and also the scientific advances in computer vision, pattern recognition, and machine learning, several biometric modalities have been largely applied to person recognition, ranging from traditional fingerprint to face, to iris, and, more recently, to vein and blood flow. Simultaneously, various spoofing attacks.

A biometric security system acting at the sensor level attacks. The latter includes all the remaining seven points of attacks and requires different levels of knowledge about the system, e.g., the matching algorithm used, the specific feature extraction procedure, database access for manipulation, and also possible weak links in the communication channels within the system.

Given that the most vulnerable part of a system is its acquisition sensor, attackers have mainly focused on direct spoofing. This is possibly because a number of biometric traits can be easily forged with the use of common apparatus and consumer electronics to imitate real biometric readings (e.g., stampers, printers, displays, audio recorders). In response to that, several biometric spoofing benchmarks have been recently proposed, allowing researchers to make steady progress in the con-ception of anti-spoofing systems. Three relevant modalities in which spoofing detection has been investigated are iris, face, and fingerprint.

In general, we expect AO to adapt the architecture to the problem in hand and FO to model important stimuli for discriminating fake and real biometric samples. We evaluate AO and FO not only in separate, but also in combination, i.e., architectures learned with AO are used for FO as well as previously known good performing architectures are used

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

with random filters. This explains the crossing dotted lines in the design flow of Fig 1. As our experiments show, the benefits of evaluating AO and FO apart and later combining them to build anti-spoofing systems are twofold. First, it enables us to have a better comprehension of the interplay between these approaches, something that has been largely underexplored in the literature of convolutional networks. Second, it allows us to build systems with outstanding performance in all nine publicly available benchmarks considered in this work.

II. LITERATURE SURVEY

[1] C. Rathgeb and A. Uhl, The fuzzy commitment scheme has been leveraged as a means of biometric template protection.
Binary templates are replaced by helper data which assist the retrieval of cryptographic keys. Biometric variance is overcome by means of error correction while authentication is performed indirectly by verifying key validities. A statistical attack against the fuzzy commitment scheme is presented. Comparisons of different pairs of binary biometric feature vectors yield binomial distributions, with standard deviations bounded by the entropy of biometric templates. In case error correction consists of a series of chunks helper data becomes vulnerable to statistical attacks. Error correction codewords are bound to separate parts of a binary template among which biometric entropy is dispersed. As a consequence, chunks of the helper data are prone to statistical significant false acceptance. In experiments the proposed attack is applied to different iris-biometric fuzzy commitment schemes retrieving cryptographic keys at alarming low effort.

[2] A. F. Sequeira, H. P. Oliveira, J. C. Monteiro, J. P. Monteiro, and J. S. Cardoso, Biometric systems based on iris are vulnerable to several attacks, particularly direct attacks consisting on the presentation of a fake iris to the sensor.
The development of iris liveness detection techniques is crucial for the deployment of iris biometric applications in daily life specially in the mobile biometric field. The 1st Mobile Iris Liveness Detection Competition (MobILive) was organized in the context of IJCB2014 in order to record recent advances in iris liveness detection. The goal for (MobILive) was to contribute to the state of the art of this particular subject. This competition covered the most common and simple spoofing attack in which printed images from an authorized user are presented to the sensor by a non-authorized user in order to obtain access. The benchmark dataset was the MobBIOfake database which is composed by a set of 800 iris images and its corresponding fake copies (obtained from printed images of the original ones captured with the same handheld device and in similar conditions). In this paper we present a brief description of the methods and the results achieved by the six participants in the competition.

[3] N. Erdogmus and S. Marcel, The problem of detecting face spoofing attacks (presentation attacks) has recently gained a well-deserved popularity.
Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. In this paper, we inspect the spoofing potential of subject-specific 3D facial masks for 2D face recognition. Additionally, we analyze Local Binary Patterns based countermeasures using both color and depth data, obtained by Kinect. For this purpose, we introduce the 3D Mask Attack Database (3DMAD), the first publicly available 3D spoofing database, recorded with a low-cost depth camera. Extensive experiments on 3DMAD show that easily attainable facial masks can pose a serious threat to 2D face recognition systems and LBP is a powerful weapon to eliminate it.

[4] Biometrics in Abc: Counter-Spoofing Research
Automated border control (ABC) is concerned with fast and secure processing for intelligence-led identification.
Advantages
It indicates that the new developing trend is fusion of multiple biometrics against spoofing attacks.
Disadvantages
Ideal ABC may have a nature of non-intrusive, efficiency, and effectiveness.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

[5] Fake Biometric Detection for Iris, Fingerprint and Face Recognition

To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures.

Advantages

Novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts.

Disadvantages

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake.

III. METHODOLOGY AND MATERIALS

3.1 SUPPORT VECTOR MACHINE (SVM)

In machine learning, support vector machines (SVMs, also support vector networks[1]) are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked for belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on.

Architecture

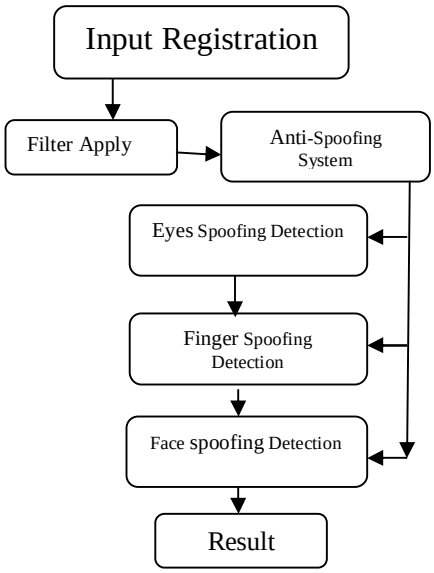

Fig: 3.1

3.2 Specular Reflection Features

Specular reflection component image has been widely used for specular reflection removal and face illumination normalization. In this paper, we separate the specular reflection component Is from an input face image or video frame utilizing an iterative method (with 6 iterations) proposed in , which assumes that the illumination is

From a single source, of uniform color, and not over-saturated. Given that most of the face images (in the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Idiap, CASIA, and MSU databases) are captured indoors under relatively controlled illumination, these three assumptions are reasonable. Illustrate the difference between the specular reflection components extracted from a genuine face and the corresponding spoof face.

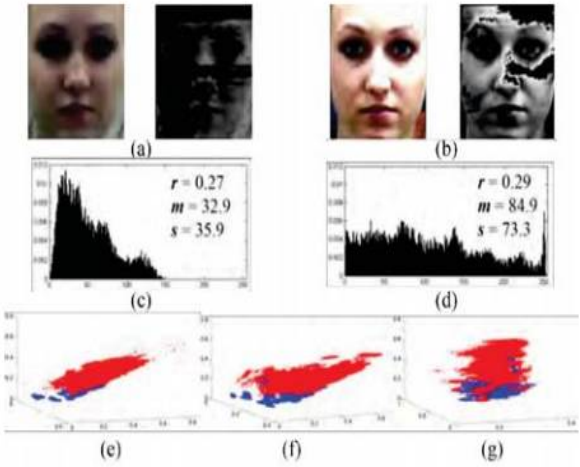

Fig: 3.2

3.3 Color Diversity Features

Another important difference between genuine and spoof faces is the color diversity. In particular, genuine faces tend to have richer colors. This diversity tends to fade out in spoof faces due to the color reproduction loss during image/video recapture. In this paper, we follow the method used in [35] to measure the image color diversity. First, color quantization (with 32 steps in the red, green and blue channels, respectively) is performed on the normalized face image. Two measurements are then pooled from the color distribution: i) the histogram bin counts of the top 100 most frequently appearing colors, and ii) the number of distinct colors appearing in the normalized face image. The dimensionality of the color diversity feature vector is 101.

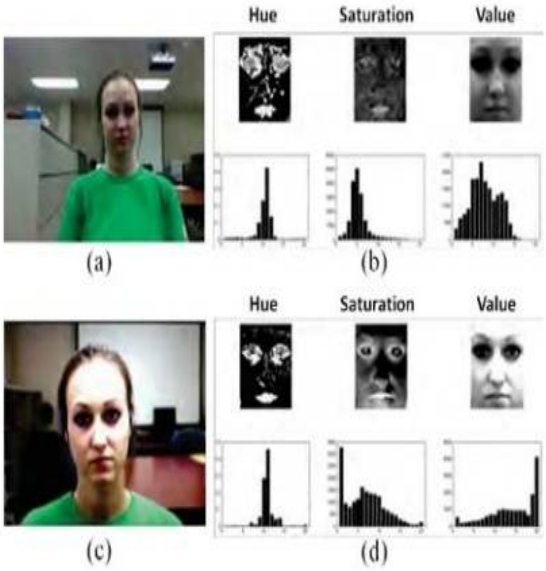

Fig:3.3

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

IV. RESULT AND DISSCUISION

The literature mostly deals with the face spoofing detection problem through texture patterns (e.g., LBP-like detectors), acquisition telltales (noise), and image quality metrics.

- Network architecture in this context is usually determined by previous knowledge of related problems
- This approach assumes little a priori knowledge about the problem, and is an area of research in deep learning that has been successful in showing that the architecture.
- Fingerprint spoofing attack detection task is still an open problem with results still far from a perfect classification rate.
- The most vulnerable part of a system is its acquisition sensor, attackers have mainly focused on direct spoofing.
- I notice that most of the groups approach the problem with hard-coded features sometimes exploring quality metrics related to the modality (e.g., directionality and ridge strength), general texture patterns (e.g., LBP-, MBLTP-, and LPQ-based methods), and filter learning through natural image statistics.

4.1. Preprocessing

A few basic preprocessing operations were executed on face, Iris and fingerprint images in order to properly learn representations for these benchmarks. This preprocessing led to images with sizes as presented in Table II and are described in the next two sections.

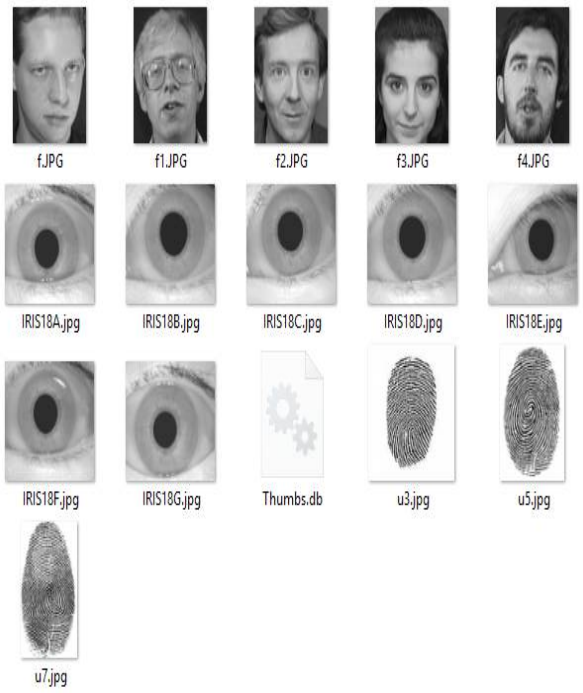

Fig: 4.1 to collect the original face, finger and iris images for store the database.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

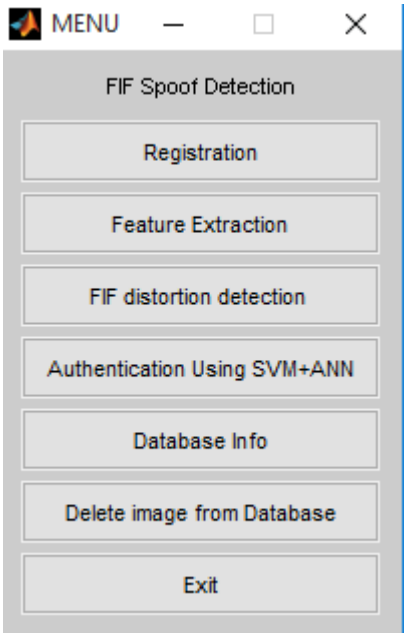

Fig: 4.2 to get menu form after preprocessing

4.2. Iris Spoofing

Iris is one such unique modality which, due to variations in iris texture, provides tremendous discriminability among different subjects and therefore is one of the most accurate approaches for recognition. Daugman proposed the first successful algorithm based on iris codes which are being used by several commercial iris technologies and applications. Thereafter, several algorithms are proposed to advance the state-of-art in iris recognition.

Iris spoofing is a mechanism by which one can obfuscate or impersonate the identity of an individual. Listed below are several easy (non-surgical) ways of spoofing an iris recognition system:

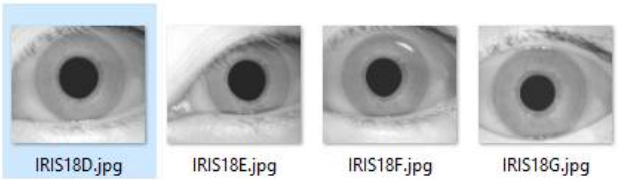

Fig: 4.3 To registered iris image for users from database

1) Pupil dilation: Pupil dilation can occur due to illumination variations, alcohol (substance) consumption, and medicine. As shown by Hollingsworth et al., large pupil dilation can cause iris patterns to be unrecognizable.
2) Textured contact lenses: Several researchers have shown that a colored textured contact lens can block the actual iris patterns and confuse an iris recognition system. Inter-class and intra-class similarities are significantly affected by colored textured contact lenses. Similarly, a lens with a painted iris obfuscates the actual eye patterns and creates a different appearance which is unseen by the iris recognition systems.
3) Print attack: Presenting a printed image of an iris to the scanner/system can help impersonating one's identity. With appropriate printer and paper combination, the quality of printed iris can be substantial enough to mislead an iris recognition system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

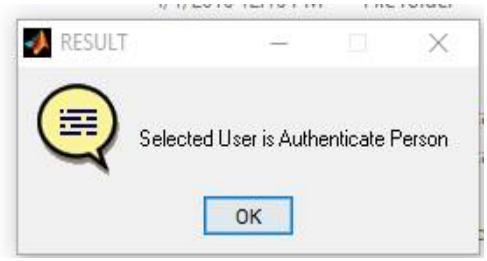

Fig:4.4 Selected user is autherised

Fig: 4.5 selected users is not authorized

4.3. Face Spoofing Detection

In this dissertation, we address the problem of face spoof detection, particularly in a cross-database scenario. While most of the published methods use motion or texture based features, we propose to perform face spoof detection based on Image Distortion Analysis (IDA). Four types of IDA features (specular reflection, blurriness, color moments, and color diversity) have been designed to capture the image distortion in the spoof face images. The four different features are concatenated together, resulting in a 121-dimensional IDA feature vector. An ensemble classifier consisting of two constituent SVM classifiers trained for different spoof attacks is used for the classification of genuine and spoof faces.

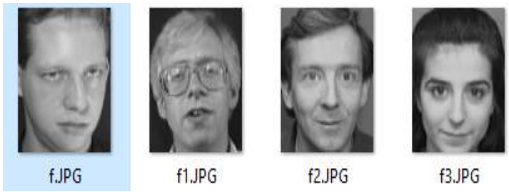

Fig: 4.6 to registered face image for users from database

Due to the intrinsic data-driven nature of texture based methods, they can be easily over-fitted to one particular illumination and imagery condition and hence do not generalize well to databases collected under different conditions.

4.4. Fingerprint Spoofing

Fingerprint distortion detection can be viewed as a two-class classification problem. We used the registered ridge orientation map and period map as the feature vector, which is classified by a SVM classifier.

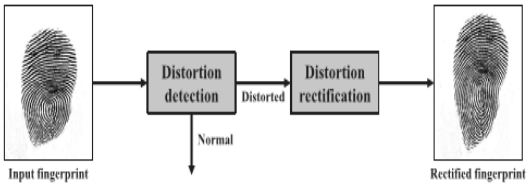

Fig: 4.7 Fingerprint spoofing

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

4.4.1 Reference Fingerprints

In order to learn statistics of realist fingerprint distortion, we collected a distorted fingerprint database called Tsing-hua distorted fingerprint database. A FTIR fingerprint scan-ner with video capture functionality was used for data collection.

Fig: 4.8 to registered iris image for users from database

Note that there are no common fingerprints between training and testing data. A large number of references are used in order to properly register fingerprints of various pattern types, while distorted fingerprints are also used as references in order that new distorted fingerprints can be properly registered.

A reference fingerprint is registered based on its finger center and direction. For fingerprints whose core points can be correctly detected by a Poincareindex based algorithm, the upper core point is used as the finger center. For arch fingerprints and those fingerprints whose upper core points are not correctly detected, we manually estimate the center point.

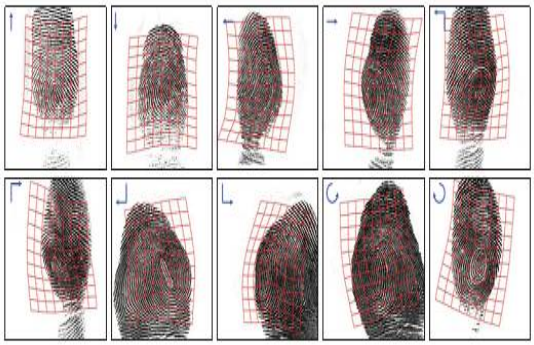

Fig: 4.9 reference Finger Print

4.5. Evaluation and Implementation

We first evaluate the proposed distortion detection algorithm. Then, we evaluate the proposed distortion rectification algorithm by performing matching experiments on three databases. Finally, we discuss the impact of the number of reference iris, fingerprints, and face on distorted iris, fingerprints, face rectification.

The input images to Veri-Finger in the three experiments are original iris, fingerprints, face, rectified iris, fingerprints, face by Senior and Bolle approach, and rectified iris, fingerprints, face by the proposed algorithms, respectively. No impostor matches were conducted because the matching score of VeriFinger is linked to the false accept rate (FAR).

1FVC2006 DB2_A was used to examine whether distortion rectification may have negative impact on matching accuracy in situations where distorted iris, fingerprints, face are absent or scarce. The distorted subset of FVC2004 DB1 consists of 89 distorted iris, fingerprints, face and mated normal iris, fingerprints, face. It was separately tested in order to clearly evaluate the contribution of distortion rectification to matching distorted iris, fingerprints, face alone.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

V. CONCLUSION AND FUTURE WORK

Our networks use classic convolution operations that can be viewed as linear and non-linear image processing operations. When stacked, these operations essentially extract higher level representations, named multiband images, whose pixel attributes are concatenated into high-dimensional feature vectors for later pattern recognition.

False non-match rates of fingerprint matchers are very high in the case of severely distorted face spec. This generates a security hole in automatic fingerprint recognition systems which can be utilized by criminals and terrorists. For this reason, it is necessary to develop a fingerprint distortion detection and rectification algorithms to fill the hole.

FUTURE WORK

For future work, we intend to evaluate such datasets using the proposed approaches here and also consider other biometric modalities such as palm, vein, and gait. Finally, it is important to take all the results discussed herein with a grain of salt. We are not presenting the final word in spoofing detection. In fact, there are important additional research that could finally take this research another step forward. We envision the application of deep learning representations on top of pre-processed image feature maps (e.g., LBP-like feature maps, acquisition-based maps exploring noise signatures, visual rhythm representations, etc.). With an n-layer feature representation, we might be able to explore features otherwise not possible using the raw data. In addition, exploring temporal coherence and fusion would be also important for video-based attacks.

REFERENCES

[1] C. Rathgeb and A. Uhl, "Attacking iris recognition: An efficient hill-climbing technique," inProc. IEEE/IAPR 20th Int. Conf. Pattern Recog-nit. (ICPR), Aug. 2010, pp. 1217–1220.
[2] C. Rathgeb and A. Uhl, "Statistical attack against iris-biometric fuzzy commitment schemes," inProc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2011, pp. 23–30.
[3] J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection," Database, vol. 1, no. 3, pp. 1–8, 2007.
[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minu-tiae matching strength," in Audio- and Video-Based Biometric Person Authentication. Berlin, Germany: Springer-Verlag, 2001, pp. 223–228.
[5] A. F. Sequeira, H. P. Oliveira, J. C. Monteiro, J. P. Monteiro, and J. S. Cardoso, "MobILive 2014—Mobile iris liveness detection competition," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB), Sep./Oct. 2014, pp. 1–6. [Online]. Available: http://mobilive2014. inescporto.pt/
[6] K. W. Bowyer and J. S. Doyle, "Cosmetic contact lenses and iris recognition spoofing," Computer, vol. 47, no. 5, pp. 96–98, May 2014.
[7] D. Yadav, N. Kohli, J. S. Doyle, R. Singh, M. Vatsa, and K. W. Bowyer, "Unraveling the effect of textured contact lenses on iris recognition," IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, pp. 851–862, May 2014.
[8] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," inProc. Int. Conf. Biometrics Special Interest Group (BIOSIG), 2012, pp. 1–7.
[9] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," inProc. IEEE 6th Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS), Sep./Oct. 2013, pp. 1–6.
[10] L. Ghiani et al., "LivDet 2013—Fingerprint liveness detection compe-tition," in Proc. Int. Conf. Biometrics (ICB), 2013, pp. 1–6. [Online].Available: http://prag.diee.unica.it/fldc/
[11] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNetclas-sification with deep convolutional neural networks," in Advances in Neural Information Processing Systems. Red Hook, NY, USA: Curran & Associates Inc., 2012.
[12] D. C. Cire¸san, U. Meier, J. Masci, and J. Schmidhuber, "Multi-column deep neural network for traffic sign classification,"NeuralNetw., vol. 32, pp. 333–338, Aug. 2012.
[13] J. Ouyang and X. Wang, "Joint deep learning for pedestrian detection," in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), 2014, pp. 2056–2063.
[14] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," in Proc. IEEE Int. Conf. Comput. Vis. Pattern Recognit., Jun. 2014, pp. 1701–1708.
[15] N. Pinto, D. Doukhan, J. J. DiCarlo, and D. D. Cox, "A high-throughput screening approach to discovering good forms of biologically inspired visual representation,"PLoSComput. Biol., vol. 5, no. 11, p. e1000579, 2009.
[16] J. Bergstra and Y. Bengio, "Random search for hyper-parameter opti-mization,"J.Mach.Learn.Res., vol. 13, no. 1, pp. 281–305, 2012.
[17] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," Proc. IEEE, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.
[18] A. M. Saxe, P. W. Koh, Z. Chen, M. Bhand, B. Suresh, and A. Y. Ng, "On random weights and unsupervised feature learning," inProc. 28th Int. Conf. Mach. Learn., 2011, pp. 1–8.
[19] Presentation Attack Detection Algorithm For Face And Iris Biometrics (R. RaghavendraChristoph Busch Norwegian Biometric Laboratory, Gjøvik University College, Norway)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

[20]Fake Biometric Detection to Iris, Fingerprint Using Image Quality Assessment (Ms. Kavita H. Waghmode M.E. Student, Signal Processing, BSCOER, Narhe, Pune, India)
[21] Biometrics In Abc: Counter-Spoofing Research (Wei, H., Chen, L. and Ferryman, J. (2013) Biometrics in ABC: counter-spoofing research.)
[22] Fake Biometric Detection For Iris, Fingerprint And Face Recognition(MohdMujeed Uddin1 ,S.V Altaf2 ,Abdul Wasay Mudassir3 MohdMujeed Uddin1 ,M.Techstudent,ECEDepartment,Lords Institute of Engineering and Technology)