ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

BIOMETRIC DECEIT DETECTION FOR SECURE AUTHENTICATION USING DEEP LEARNING

Udhaya.M 1* , B. Muthu Kumar 2 , Kavitha 3 , S.Prabhakaran 4

1, 3Department of Computer Science, Sakthi College of Arts and Science for Women, TN, India

2 Professor, Department of CSE, Syed Ammal Engineering College, Ramanathapuram, TN, India

4 Department of Information Technology, Kathir College of Engineering

*Corresponding Author: mailto: m.udhaya21@gmail.com

Abstract— Biometrics systems are playing an important role in personal, national and global security to improve person recognition and authentication. However, the deceiving attacks are occurred, it can be overcome by biometric systems. The people are heedless about biometric deceit sensor to derive outstanding deceit detection systems. They are iris, face, and fingerprint techniques based on the approaches of deep learning [13]. The first approach includes of learning each patch in convolutional network architectures and through back propagation the second approach concentrates on learning the weights [18] of the network. The nine biometric deceit specifications each one containing real and fake [20] samples of a given biometric modality and attack type and learn deep representations for each specification by combining and contrasting the two learning approaches. This plan provides better result from the eight out of nine specifications. The outcomes indicate that deceit [22] detection systems based on convolutional networks can be resilient to attacks already known and possibly adapted, with little effort, to image-based attacks.

Index Terms— filter weights learning, back-propagation, deceit detection.

I. INTRODUCTION

BIOMETRICS are used for access control, espionage and also in every security systems by allowing person recognition and authentication based on the features of human. The biometric techniques have been widely applied to person recognition, ranging from traditional fingerprint to face [19], to iris and recently, to vein and blood flow for data acquisition, storage and processing, and also the scientific advances in computer vision, pattern recognition, and machine learning due to technological improvements.

There are various methods to deceit a biometric system. Indeed, previous works show eight different points of attack that can be divided into two main categories: direct and indirect attacks. The possibility to generate synthetic biometric samples is the first exposure of biometric security sensors. The final comprises all the remaining seven attacks and statutory different proportions 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.

This is possibly because a number of biometric traits can be easily forged with the use of common equipments and consumer electronics to emulate real biometric readings. Examples are stampers, printers,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

displays, audio [4] recorders. The biometric deceit specifications allowed researchers to make steady advance in the beginning of anti-deceit systems. The deceit detection has been investigated are iris, face, and fingerprint techniques. Specifications share the common characteristic of image or video based.

The success of an anti-deceit method is based on the design. It is able to capture acquisition telltales left by specific attacks based on the systems rely on expert knowledge. Small changes in the attack could require the redesign of the entire system.

In this paper, we do not focus on custom-tailored solutions. Instead, inspired by the Deep Learning's success in various tasks, and by the ability of the technique to leverage data concentrates on two general-purpose approaches to build image-based anti-deceit systems with convolution networks for several attack types. [6] proposed a system in which OWT extracts wavelet features which give a good separation of different patterns. Moreover the proposed algorithm uses morphological operators for effective segmentation. From the qualitative and quantitative results, it is concluded that our proposed method has improved segmentation quality and it is reliable, fast and can be used with reduced computational complexity than direct applications of Histogram Clustering. The main advantage of this method is the use of single parameter and also very faster. While comparing with five color spaces, segmentation scheme produces results noticeably better in RGB color space compared to all other color spaces.

The Filter optimization [16] (FO) and Architecture Optimization (AO) are presented on the left and right high-lighten as blue and red.

The practical outcome strongly indicates that convolutional [11] networks can be readily used for brawny deceit detection. In fact, in the research field the data-driven solutions based on deep representations is a valuable direction, allowing the construction of systems with little effort to image-based attack types. The remaining works are classified into five sections. Section II enlightens the previous anti-deceit systems for the three biometric techniques discussed in this paper, while Section III describes the methodology adopted for architecture optimization (AO) and filter optimization (FO) while Section IV presents experiments, results, and comparisons with state-of-the-art methods. Finally, Section V concludes the paper and discusses some possible future works.

II. RELATED WORKS

[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

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

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 [5] 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 deceit 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 specification 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 deceit attacks (presentation attacks) has recently gained a well-deserved popularity.

Mainly focusing on 2D [9] 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 deceit material in front of the sensor. In this paper, we inspect the deceit 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 deceit 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.

III. METHODOLOGY

3.1 SUPPORT VECTOR MACHINE (SVM)

A Support Vector Machine (SVM) is used to define a separating hyperplane. The output of the hyperplane is classified into two classes. They are horizontal and vertical hyperplanes. The SVM algorithm is used to find the hyperplane. It gives the largest minimum distance. The distance of twice receives the name of the margin within SVM's theory. Optimal are used to separate the .hyperplane and maximize the margin data.

Nonlinear classification

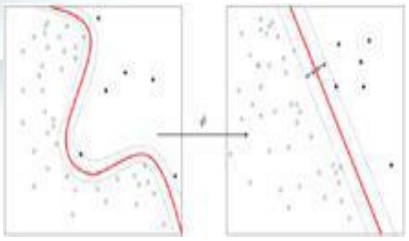

Fig: 3.1 Nonlinear

3.2 Fast Fourier Transform (FFT)

In this figure 3.2 a Fast Fourier transform (FFT) is a systematic algorithm to compute the DFT

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

for an input vector. Systematic means FFT can compute the DFT of n-element vector in O (n log n) operations contrasts to the O (n^2). FFT exists for vector length n. Parallel FFT developed for advent of parallel computing. FFT are used to represent the sequence of summations or its factorization of transform matrix. FFT is used to transform the function of time into function of frequency. It mainly supports to identify the timing dependent. FFT's major work is to breakdown the complicated signal and converts into simple waves.

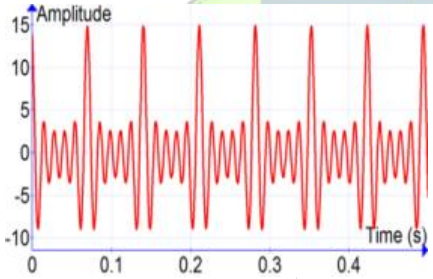

Fig: 3.2 Fast Fourier Transform

Architecture

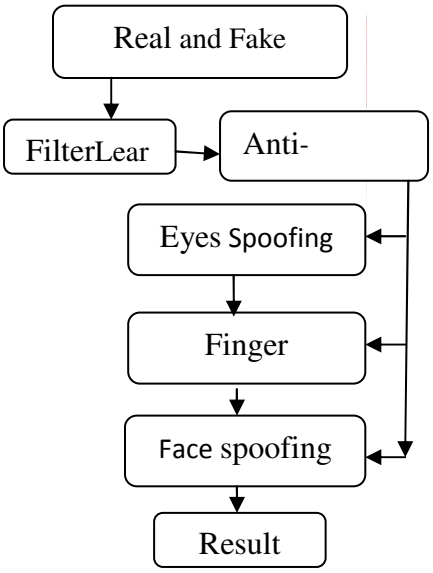

Fig: 3.3 Architecture

3.3 Specular Reflection Features

In figure 3.4 shows specular reflection is like a mirror reflection of light and the light reflects in a single incoming direction and into a single outgoing direction. It reflects the light in the entire same angle. Lights are used to reflect in three possible outcomes such as absorption, transmission and reflection. The light reflected at a definite angle is from a smooth surface. The light reflections are depending upon the smooth surfaces or texture surfaces. To remove specular reflection and normalizing face gleam, specular reflection component image is used. The input face image or video used to separate the technique which is specular reflection component. The assumption is gleam comes from a single source of same color and not over saturated. The face [14] images are captured indoors under relatively controlled gleam and it presents the difference between the genuine face of a specular reflection components and the corresponding deceit face.

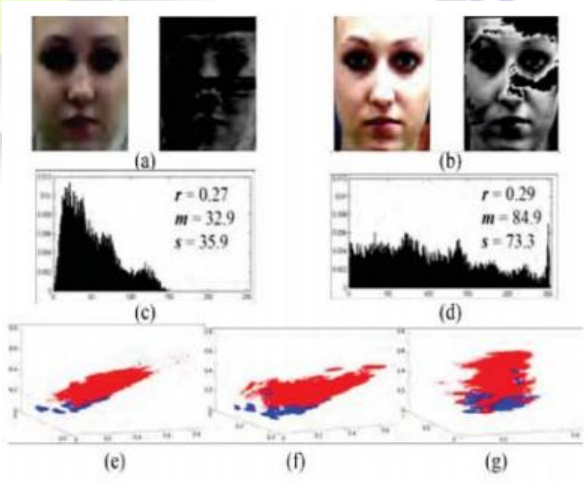

Fig: 3.4 Specular Reflection

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

3.4 Color Contrast Features

Another important difference between genuine and deceit faces is the color contrast. Genuine faces have opulent colors. This contrast tends to dwindle out in deceit faces due to the color proliferation loss during image/video reseize. In this paper, we follow the method used to measure the image color contrast. Color with 32 steps in the RGB channels is performed on the normalized face image. In this figure 3.5 shows two measurements are then obtained from the color distribution: i) the top 100 most frequently appearing colors, and ii) the number of unique colors appearing in the normalized face image. The dimensionality of the color contrast feature vector is 101.

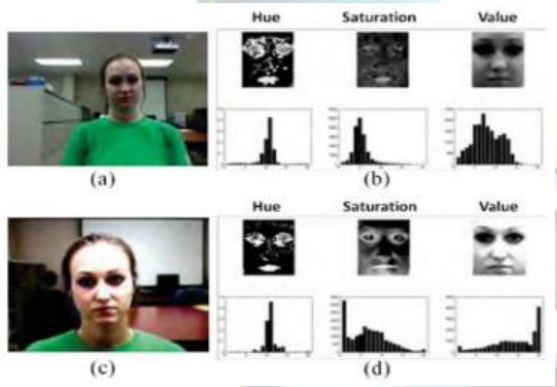

Fig:3.5 Color Contrast

IV. RESULT AND DISSCUISION

The information deals with the face deceit detection problem through texture patterns and image quality metrics.

- By considering the previous problems, Network architecture (figure 3.3) in designed.
- To reduce the problems, deep learning technique is assumed.
- Fingerprint deceit attack detection is a huge problem and the outcome is far away from a perfect classification rate.
- The acquisition sensor is the unshielded [3] part of a system and the attackers mostly focuses on deceit directly.

4.1. Preprocessing

The preprocessing testing was executed on face, Iris [2] and fingerprint images to study the representations properly. In this figure 4.1 & 4.2 preprocessing lead to images with sizes.

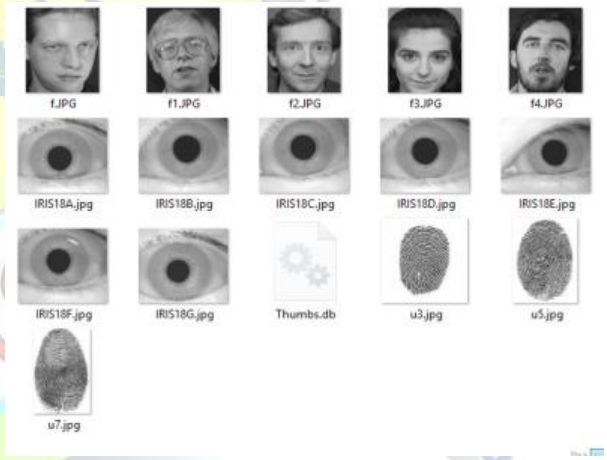

Fig: 4.1 To collect the original face, finger and iris images for store the database.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

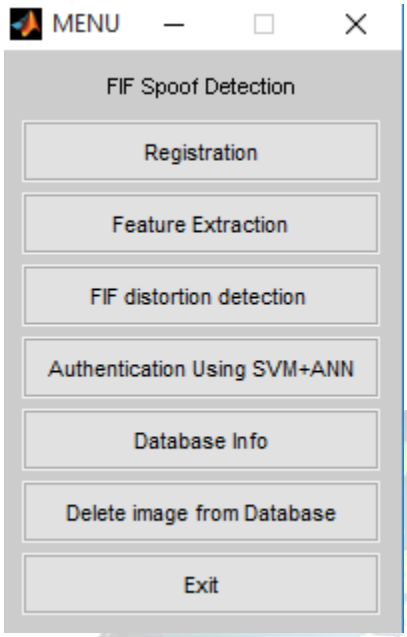

Fig: 4.2 To get menu form after preprocessing

4.2. Iris Deceit Detection

In figure 4.3 iris [1] is a unique modality and it generates the accurate result for recognition [17]. The first algorithm was proposed by Daugman based on iris codes which are used in iris technologies and applications. The several algorithms are also proposed to advance the state-of-art in iris recognition.

Iris deceit is a technique by which one can muddle or mock the identity of a sole. The ways of deceit an iris recognition system is discussed below:

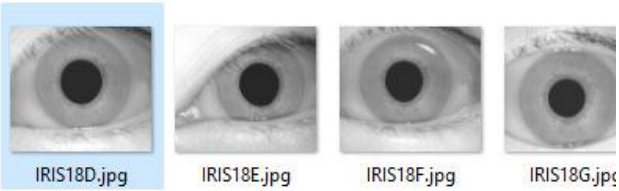

Fig: 4.3 To registered iris image for users from database

1) Pupil dilation: Pupil dilation can occur due to gleam 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 [7] 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.

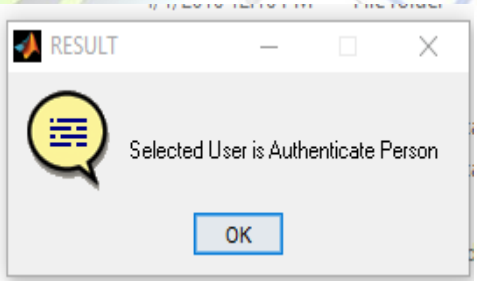

Fig:4.4 Selected user is autherised

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

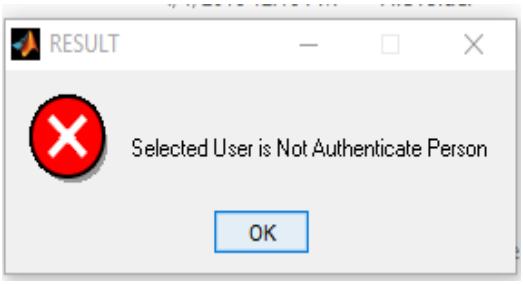

Fig: 4.5 Selected users is not authorized

4.3. Face Deceit Detection

In this dissertation, the problem of face deceit detection, particularly in a cross-database scenario is reviewed. The proposed method is to perform face [8] deceit detection based on Image Distortion Analysis (IDA). The IDA features are classified into specular reflection, blurriness, color moments, and color contrast have been designed to capture the image distortion. The 121-dimensional IDA feature vector is resulted from the four different features joined together. A troupe classifier consists of two constituent SVM features used for the classification of genuine and deceit faces.

Fig: 4.6 To registered face image for users from database

Due to the innate data-driven nature of texture based methods, they can be easily over-fitted to one particular gleam and imagery condition. It does not generalize to databases collected under disparate conditions.

4.4. Fingerprint Deceit Detection

Fingerprint [10] [22] distortion detection problem are classified into two types such as the registered ridge orientation map and period map as the feature vector, which is classified by a SVM classifier.

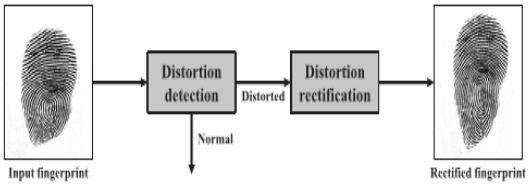

Fig: 4.7 Fingerprint deceit

4.4.1 Reference Fingerprints

To study the fingerprint (figure 4.8) distortion statistics, Tsinghua distorted fingerprint database is used. For data collection, a FTIR fingerprint scanner with video capture functionality was utilized.

Fig: 4.8 To registered iris image for users from database

In this figure 4.9 the fingerprints between training and testing data are different. A large number of references are used to register the various patterns of fingerprints properly. Distorted fingerprints are also used as reference.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

Based on the finger's center and direction, a reference fingerprint is registered. The accurate fingerprints results are generated by a Poincare index based algorithm. The upper core point is used as the finger center. For arch fingerprints upper core points are not correctly detected and the centre point is manually estimated.

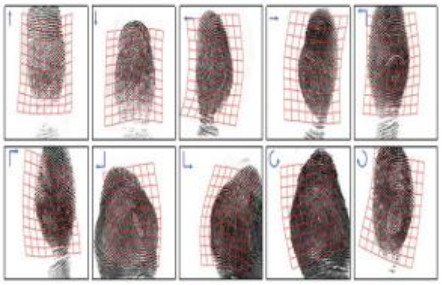

Fig: 4.9 Reference Finger Print

4.5. Evaluation and Implementation

The proposed distortion detection algorithm and the distortion rectification algorithm is evaluated by performing matching experiments on three databases. Finally, we discuss the impact of the number of reference iris, fingerprints, face on distorted iris and face rectification.

The input images are given to Veri-Finger technique. The three experiments are original iris, fingerprints, face, rectified iris, fingerprints, face by Senior and Bolle approach, and rectified iris, fingerprints, face. No burglar matches were conducted because the matching score of Veri-Finger 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 or not in distorted iris, fingerprints, face. The distorted subset of FVC2004 DB1 consists of 89 distorted iris, fingerprints, face and pairing normal iris, fingerprints, face. To clearly evaluate the contribution of distortion rectification to matching distorted iris, fingerprints, face, it was tested separately

V. CONCLUSION & FUTURE WORK

5.1 CONCLUSION

Our networks use classic convolution operations that can be viewed as linear and non-linear image processing operations. The operations are essentially extracted from higher level representations and named as multiband images, whose pixel attributes are joined into high-dimensional feature vectors for later pattern recognition. False non-match rates of fingerprint matchers are very high. By using the security hole in automatic fingerprint recognition system the criminals and terrorists used it in an illegal manner. For this reason, it is necessary to develop a fingerprint distortion detection and rectification algorithms to fill the hole.

Face deceit detection include

i. Understand the characteristics and requirements for face deceit detection.

ii. By considering the user demographics (age, gender, and race) and ambient gleam a large and representative database is collected.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

iii. To develop robust, effective, and efficient features (e.g., through feature transformations) for the network.

iv. Consider user-specific training for face deceit detection.

By using the proposed method enhance the biometric modalities such as palm, vein, and gait. In fact, there is an additional research that could take to next step. We imagine 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 [15] 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] Christo Ananth, A.S.Senthilkani, Praghash.K, Chakka Raja.M., Jerrin John, I.Annadurai, "Overlap Wavelet Transform for Image Segmentation", International Journal of Electronics Communication and Computer Technology (IJECCT), Volume 4, Issue 3 (May 2014), pp-656-658

[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-deceit," inProc. Int. Conf. Biometrics Special Interest Group (BIOSIG), 2012, pp. 1–7.

[9] N. Erdogmus and S. Marcel, "Deceit in 2D face recognition with 3D masks and anti-deceit 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

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

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)

[20]Fake Biometric Detection to Iris, Fingerprint Using Image Quality Assessment (Ms. Kavita H. Waghmode M.E. Student, Signal Processing, BSCOER, Narhe, Pune, India)

M.Udhaya received her MSC(IT) degree from Sri Nagalakshmin Ammal College for Science, Pappunayakanpatti, India in 2015. Now she is currently working toward the M.Phil degree at Sakthi Arts & Science College for women, Oddanchtram, India. Her main research interests include Image Processing, Network Security.

B. Muthu Kumar, Professor, Department of CSE, Syed Ammal Engineering College, Ramanathapuram, TN, India

Kavitha, Professor, Department of Computer Science, Sakthi College of Arts and Science for Women, TN, India

S.Prabhakaran, Department of Information Technology, Kathir College of Engineering, Now he is currently working in Ascox Techno Soft at Madurai, India. Him main research interests include Image Processing, Network Security, Cloud Computing.