SEFL: Selective Ensemble Fuzzy Learner for Cognitive Detection of Bio-Modality Spoofing in MCPS

Nishat I Mowla*, Inshil Doh**, Kijoon Chae*

*Department of Computer Science and Engineering, Ewha Womans University, 52, Ewhayeodaegil, Seodaemungu, Seoul, 03760, Korea

**Department of Cyber Security,Ewha Womans University, 52, Ewhayeodaegil, Seodaemungu, Seoul, 03760, Korea Name

nishat.i.mowla@gmail.com, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

***Abstract*—User authentication in a Medical Cyber Physical Systems (MCPS) can be effectively done using biometric features. Biometric features, widely used for user authentication, are equally important to national and global technology systems. Biometric features, such as face, iris, fingerprint, are commonly used while more recently palm, vein and gait are also getting attention. To fail the traditional biometric detection systems, various spoofing approaches have also been developed over time. Among various methods, image synthesis with play-doh, gelatin, ecoflex etc. are some of the more common ways for spoofing bio-modalities. Success of traditional detection systems are related to custom tailored solutions where feature engineering for each attack type must be developed. However, this is not a feasible process when we consider countless attack possibilities. Also, a slight change in the attack can cause the whole system to be redesigned and therefore becomes a limiting constraint. The recent success of machine learning inspires this paper to explore weak and strong learners with ensemble learning approaches using AdaBoost. In essence, the paper proposes a selective ensemble fuzzy learner approach using Ada Boost, feature selection and combination of weak and strong learners to enhance the detection of bio-modality spoofing for MCPS. Our proposal was experimented on real datasets and verified on the fingerprint and iris benchmark.**

***Keyword*—MCPS, Biometric spoofing, Spoofing Detection, Ensemble Learning, Feature selection**

I. INTRODUCTION

MEDICAL Cyber Physical Systems are a four-layer architecture which extends from users in the acquisition layer to cloudlet to cloud and then to the caregiver. As it is a sensory network composed of medical aspects, biometric features can be effectively used for user authentication. An increasing interest in the evaluation of biometric systems in recent years have been observed for user identification and authentication leveraging traditional fingerprint, iris and more recently vein, blood flow etc. In the other hand, various spoofing attacks have also been developed to defeat these systems. Given these attacks are performed in an analog domain with heavy device dependency following regular protocol, digital protection schemes such as encryption, digital signature or watermarking are unsuitable. The success of detection mechanism for such types of attacks are often linked to custom tailored solution where feature engineering plays a major role. Nevertheless, in a pool of myriad possible attacks, a slight change in the attack model can cause the whole mechanism to be redesigned to adopt the new mechanism which surely becomes a limiting constraint [1]. The past few years have witnessed the success of Deep Learning techniques such as Convolutional Neural Network (CNN) for efficient image classification and Recurrent Neural Network (RNN) for its special recurrence capabilities in contextual image recognition [2]. While high accuracy can be achieved, the computation can take long time which becomes a limiting constraint for time-critical systems such as MCPS.

Previously, we proposed a fuzzy ensemble learner based cognitive detection scheme for fingerprint spoofing in an MCPS where a selective ensemble architecture was proposed using Ada Boost and feature selection [31]. In this paper, we extend the research to more complex modality of the iris benchmark to further verify the effectiveness of the selective ensemble architecture to make the problem space simpler and enhance the overall performance. The performance of the strong learner is further substantiated with the more complex representation of the iris benchmark to provide further insight.

We discuss some of the related works in sections II. In section III we discuss our proposed mechanism and evaluation results followed by the conclusion in section IV.

Manuscript received on Jan. 15, 2018. This work is sponsored by Basic Science Research Program through the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIP), and a follow-up of the invited journal to the accepted & presented paper of the 19th International Conference on Advanced Communication Technology (ICACT2017), and Grant ID is 2016R1A2B4015899. Kijoon Chae is the corresponding author.

Chae. Kijoon. Author is with Ewha Womans University, Seoul, 120750 Korea (corresponding author to provide phone: +82-10-3726-6157; e-mail: kjchae@ ewha.ac.kr).

Mowla Nishat. Author, is with Ewha Womans University, Seoul, 120750 Korea. (e-mail: nishat.i.mowla@gmail.com).

Doh Inshil. Author is with Ewha Womans University, Seoul, 120750 Korea. (e-mail: isdoh1@ewha.ac.kr).

II. Related Works

In this section, we review anti-spoofing related work for bio-identifiable modalities focusing on fingerprint spoofing.

A. Bio-identifiable Modality Spoofing Detection

For fingerprint spoofing detection, both hardware-based (exploring extra sensors) and software-based solutions (relying only on the information acquired by the standard acquisition sensor of the authentication system) have been explored. In [3] quality measures such as ridge strength or directionality, ridge continuity, ridge clarity, and integrity of the ridge-valley structure was used as a set of features for fingerprint liveness detection. In [4], the presence of gummy fingers was explored using various methods. In [5], a method for representing all spectrum characteristics in a compact feature representation form was explored. In [6], well suited to high contrast patterns such as the ridges and valleys of fingerprints images, Weber Local Image Descriptor (WLD) for liveness detection was considered. In [7] Multi-Scale Block Local Ternary Patterns (MBLTP) was proposed as a liveness detection scheme. In [8], Binarized Statistical Image Features (BSIF) was explored which was originally proposed in [9]. According to reports in the LivDet 2013 Fingerprint Liveness Detection Competition [28], the fingerprint spoofing attack detection task remains an open problem with results still far from a perfect classification rate. Mostly 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 are heavily followed.

For iris spoofing spoofing detection, the use of Fast Fourier Transform was proposed in [10] to verify the high frequency spectral magnitude in the frequency domain for iris spoofing detection. Solutions for iris liveness detection range from hardware-based solutions [11] [12] [13] to software-based solutions relying on texture analysis for detecting an attacker using contact lenses with someone else's printed pattern [14]. Software-based solutions considering cosmetic contact lenses [15], [16], [17], [18]; pupil constriction [19]; and multi biometrics of electroencephalogram (EEG) and iris together [20] had been explored rigorously. In [21], best features are selected through sequential floating feature selection (SFFS) [22] to feed a quadratic discriminant classifier. In [23], image quality measures were explored, and three classification techniques were proposed. In [24], the previous work was extended by using a feature selection step on the features of the studied methods to obtain the "best features" and then used well-known classifiers for the decision making. In [25], iris segmentation was proposed to obtain the iris contour and feature extraction processes were adapted to the resulting non-circular iris regions. In [26], a general framework for iris image classification based on a Hierarchical Visual Codebook (HVC) encoding the texture primitives of iris images was proposed. For iris spoofing detection, features have been profoundly studied through image-quality metrics, texture patterns, bags-of-visual-words and noise artifacts.

B. Machine Learning based Bio-modality Spoofing Detection

A couple of machine learning based methods was proposed for bio-modality spoofing detection in recent years. A deep architecture based on Convolutional Neural Network using Architecture Optimization (AO) and Filter Optimization (FO) was proposed in [1]. The results were verified in three different modalities and in multiple real datasets. In [2], a combination of Recurrent Neural Network and Convolutional Neural Network was used to create a deep architecture which is context aware as well as capable of detecting high level features. Different existing datasets are used to evaluate the performance bio-identifiable modality spoofing using machine learning algorithms in many research works [1]. However, these architectures require heavy weight algorithms which cannot run fast enough without the use of GPU which incurs another level of computational cost. In [27], a lightweight Adaboost based model with k-means clustering was used to optimize detection accuracy of images. While some considered various deep and boosting algorithms, not many explored the role of features and ensemble learning in a profound way. Our proposed approach, therefore, aims to leverage low computation weak learners and moderately strong learners with boosting ensemble and feature selection for detecting fingerprint and iris benchmark spoofing detection as an authentication verification scheme in Medical Cyber Physical Systems.

III. Proposed Mechanism

Machine Learning performs various levels of learning. It has effectively explored various boosting techniques such as Ada Boost. The main idea of Ada Boost is to set a bunch of weak classifiers or learners working together to outperform a single strong learner [27]. The idea can also be verified with various weak learner architectures such as one-level Decision Tree. Boosting is also a form of ensemble learning where the output of the most efficient learner is incorporated into the final result [27]. However, there are certain features that are learned well by weak learners and certain features that are learned better by strong learners. Based on such facts, our paper is inspired to propose training light weight strong learners parallelly with the weak learners, as a combo learner, which undergoes selective ensemble learning with Ada Boost and feature selection in order to come up with the final decision algorithm. The following sub-section describes our scheme in more detail.

In our proposed scheme, the bio-modality spoofing is learned with one strong learner and one weak learner using Ada Boost. Both learners are represented in different feature selected environments. The fuzzy ensemble algorithm, then, chooses the best combination of the machine learning algorithm and feature selection value as the final decision-making algorithm. Fig 1 shows the basic workflow of our proposed fuzzy ensemble learning algorithm using Ada Boost, feature selection and strong and weak learner combinations.

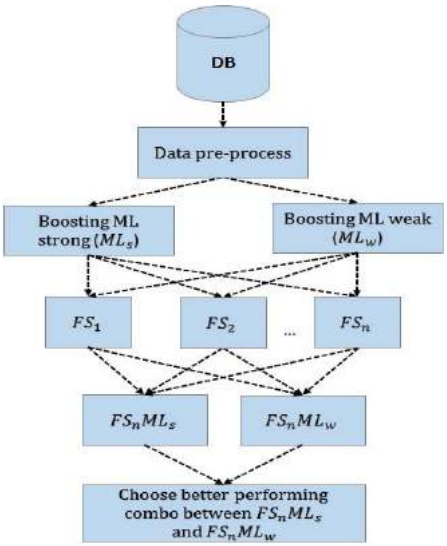

Fig. 1 Selective Ensemble Fuzzy Learning [31].

In the above figure, the DB is used to provide a two-class problem containing spoofed bio-identifiable modality and live bio-identifiable modality. The two-class problem is then learned by one strong learning algorithm and one weak learning algorithm. FS_1, FS_2, FS_n are the different feature selection environments where n is the total number of features used in the experimentation. FS_nML_s represents the best feature selected environment of the strong learning algorithm. Similarly, FS_nML_w represents the best feature selected environment of the weak learning algorithm. Finally, the best combination out of these two environments, FS_nML_s and FS_nML_w, is selected as the decision-making algorithm combination for the final decision process.

The combination of weak and strong learners with Ada Boost is an unexplored field with potential. This is because, it is believed that weak learners together can perform better but it is not explored how a moderately strong learner with lower computational overhead added to this environment could help the overall detection performance. Besides, ensemble learning is computationally expensive. Hence, selective ensemble learning is proposed which can reduce the number of features. The latter is further enhanced by introducing a feature selection methodology to aid in the selective ensemble approach.

LiveDet 2015 [28] and Warsaw [29] dataset provides different kinds of modality spoofing benchmark along with live dataset benchmark. On these different spoofing datasets, we apply our selective fuzzy ensemble learning with feature selection and Ada boost which, as discussed before, can be summarized to follow three major steps as discussed below.

***1) Fuzzy Learning*:** One strong learner and one weak learner is used to learn the spoofed and non-spoofed instances. Both learners are processed with boosting algorithm by using Ada Boost.

2) Feature Selection: This is done in two inter-linked steps. Both learners in the fuzzy learning approach is represented in different feature selected environments. It is known that best performance is not always obtained by using the most number of features but by using the most relevant features. Therefore, the best feature selection value is saved for both the weak learner and the strong learner.

3) *Combo Selection:* The feature selection value with higher accuracy, among the two best feature selection values saved in the feature selection step, is selected. Therefore, the final decision-making algorithm uses this feature selection value along with its corresponding machine learning algorithm which could either be a weak or a strong learning algorithm based on the attained accuracy.

The algorithm of our proposed selective fuzzy ensemble learner using Ada Boost and feature selection is shown below.

Algorithm 1 Selective Ensemble Fuzzy Boosted Learner

```
pre-process images to form a 2-class problem;
initialize class spoofed = 1;
initialize class live =0;
run Feature Selection algorithm;
    run classification with boosted strong learner;
    get best learner and feature selection combo, fs_x1;
    run classification with boosted weak learner;
    get best learner and features selection combo, fs_x2;
    if fs_x1 > fs_x2 then
        choose fs_x1;
    else
        choose fs_x2;
```

After pre-processing the data to form a 2-class problem where one is the spoofed class and the other is the non-spoofed class. Class spoofed is initialized as 1 and class live or non-spoofed is initialized as 0. The feature selection algorithm is run for both the strong and weak learner. The combo of the learner and feature selection is compared to find the best combo.

IV. Peroformance Evaluation

The LiveDet 2015 [28] and Warsaw dataset [29] dataset provides a set of spoofed and live biometric dataset. For our experimentation, we used the benchmark for the fingerprint and iris dataset containing spoofed and live instances. The benchmarks were pre-processed to extract features from each spoofed and live image and stored as ARFF (Attribute-Relation File Format) files.

After pre-processing the benchmarks to extract the features, a two-class problem is created containing spoofed and non-spoofed instances. We used Knime Analytics tool[30] for pre-processing the dataset and simulating the boosted strong and weak learners. Therefore, the dataset is then learned by one boosted strong learner and one boosted weak learner. For strong learner we used Naïve Bayes and for weak learner we used a One-Level Decision Tree. Fig. 4 and Fig. 5 shows our simulation of the dataset classification with the learners using Ada Boosting and feature selection.

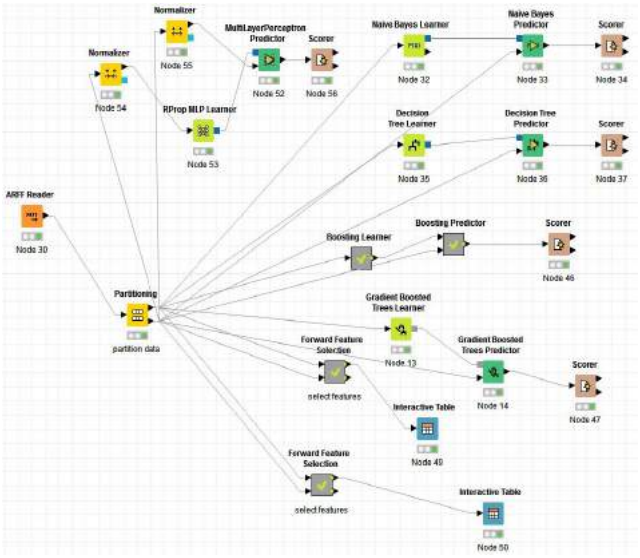

Fig. 2. Data partitioning and forwarding feature selection [31].

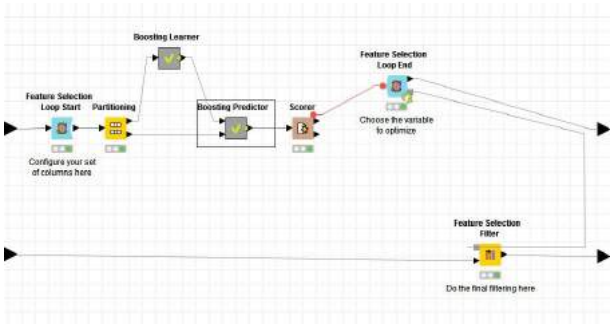

Fig. 3. Boosting Learner and Feature Selction [31].

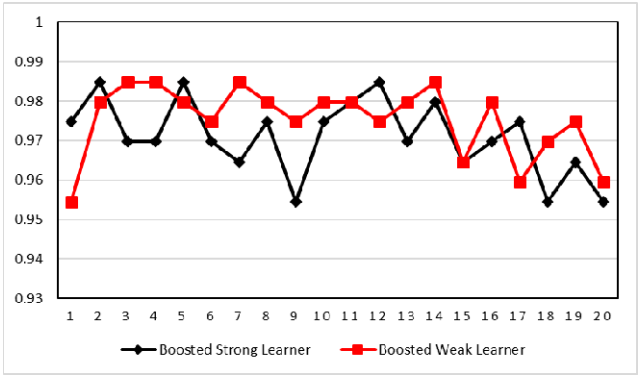

Fig. 4. Different feature selected values for Boosted Strong and Weak Learner for fingerprint benchmark.

The learning is performed for a range of feature selected environments ranging from 1-feature selection to all 20-feature selection. Fig. 4 and Fig. 5 shows the results for the selective ensemble strong boosted learner, Naïve Bayes and weak boosted learner, 1-level Boosted Decision Tree, in different feature selected environments for fingerprint and iris benchmark respectively.

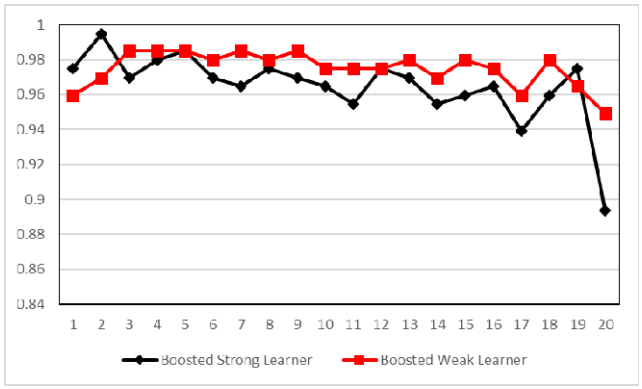

Fig. 5. Different feature selected values for Boosted Strong and Weak Learner for iris benchmark.

The combined learning of these two learners are monitored for all feature selection environment to extract the best selection values. As can be seen from Fig. 4, in terms of average accuracy, we get highest performance (98.485%) with 2,5 and 12 feature selection value for the boosted strong learner and 3,4,7 and 14 feature selection value for the boosted weak learner. Combinedly, we can get achieve highest performance with 2,3,4,5,7,12 and 14 features. From Fig. 5, we get highest performance (99.495%) with 2 features for boosted strong learner and with 3,4,5,7 and 9 features for the boosted weak learner. Thus, based on the available features and preferred algorithm between the strong and weak learner, we can choose the final combination as the decision algorithm. Table 1 summarizes a list of comparable algorithms to our proposed Selective Ensemble Fuzzy Boosted Learner algorithm.

TABLE I
BIO-MODALITY DETECTION OF FINGERPRINT BENCHMARK

Algorithm	Average Accuracy	Number of Features
Naïve Bayes	92.407	20
Decision Tree	96.418	20
Boosted Naïve Bayes	94.628	20
Boosted Decision Tree	97.278	20
Multi-Layer Perceptron	95.989	20
Selective Fuzzy	**98.485**	Min: 2
Ensemble Learner		Max: 14

TABLE II
BIO-MODALITY DETECTION OF IRIS BENCHMARK

Algorithm	Average Accuracy	Number of Features
Naïve Bayes	92.407	20
Decision Tree	96.418	20
Boosted Naïve Bayes	89.393	20
Boosted Decision Tree	94.949	20
Multi-Layer Perceptron	81.5	20
Selective Fuzzy	**99.495**	Min: 2
Ensemble Learner		Max: 2

As can be seen from the above two tables, the learning is optimum for our proposed selective ensemble fuzzy learner in terms of average accuracy metric. For fingerprint, this high performance can be achieved by the lowest feature selection using 2 features with a strong boosted learner, or the highest feature selection using 14 features with a weak boosted learner.

In this case, the highest number of features used is 14 which is still lower than the total number of features that is used by the

other algorithms. Besides 5 features and 12 features with a strong boosted learner and 3,4 and 7 features with a weak boosted learner can also be used giving the same highest accuracy of 98.485 percent. In our approach, since the number of features used will be less than the total number of features and the algorithm can alternate between a weak and moderately strong learner, the overall overhead can be significantly reduced in best cases with 2,3,4 and 5 features, moderate cases with 7 features and in worst cases with 12 or 14 features which is still lesser than the total number of features. For iris, the highest performance can be achieved by the feature selection using 2 features with a strong boosted learner. Since this feature selection alone provides the highest performance, we do not need to consider other feature selection and learner combos. As can be seen, in this case, a strong boosted learner outperforms a weak boosted learner. And since we can alternate between the strong learner and weak learner we can utilize both the learners depending on the kind of learning environment.

The performance gain of this paper is credited to the fact that learning is flexible and able to move between a moderately strong and a weak learner. While the statement, weak learners together can perform better than a strong learner holds, it is also shown that strong learners working together with weak learners can also gain promising performance in desired feature selected values. Ensemble learning is computationally expensive but, in our case, the feature selected ensemble is helping to make the problem space smaller and simpler. Thus, while the performance is improving, the overall complexity is not rising significantly.

V. Conclusion

In this paper, we have proposed a selective ensemble fuzzy learner with Ada Boost and Feature Selection in order to detect bio-identifiable modality spoofing of fingerprint and iris benchmark that can be used for authentication in a Medical Cyber Physical System. We have shown that our proposed mechanism enhances the performance of the traditional boosted learning algorithms. Our mechanism also considers a selective ensemble learning approach to reduce the overall computational overhead. In future work, we hope to apply our proposed mechanism in other bio-identifiable modality spoofing.

Acknowledgment

The work was supported by the National Research Foundation of Korea (NRF) funded by the Korea government (MSIP) (2016R1A2B4015899). Kijoon Chae is corresponding author

References

[1] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. P. A. X. Falcao, and A. Rocha. "Deep representations for iris, face, and fingerprint spoofing detection." *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 864-879, 2015.

[2] M. Liang, and X. Hu. "Recurrent convolutional neural network for object recognition." *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 3367-3375. 2015.

[3] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Fingerprint liveness detection based on quality measures," *in Proc. Int. Conf. Biometrics, Identity, Secur. (BIdS)*, pp. 1–8, 2009.

[4] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generat. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, 2012.

[5] L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," *in Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, Nov. 2012, pp. 537–540.

[6] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint liveness detection based on weber local image descriptor," *in Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl.*, pp. 46–50, Sep. 2013.

[7] X. Jia et al., "Multi-scale block local ternary patterns for fingerprints vitality detection," *in Proc. IAPR Int. Conf. Biometrics (ICB)*, pp. 1–6, 2013.

[8] L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection using binarized statistical image features," *in Proc. IEEE Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, pp. 1–6, Sep./Oct. 2013.

[9] J. Kannala and E. Rahtu, "BSIF: Binarized statistical image features," *in Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, pp. 1363–1366, Nov. 2012.

[10] J. Daugman, "Recognizing persons by their iris patterns," *in Biometrics:Personal Identification in Networked Society*, Boston, MA, USA:Kluwer, pp. 103-121, 1999.

[11] C. Lee, K. R. Park, and J. Kim, "Fake iris detection by using purkinje image," *in Advances in Biometrics (Lecture Notes in Computer Science), New York, NY, USA: Springer-Verlag*, vol. 3832, pp. 397-403, 2005.

[12] A. Pacut and A. Czajka, "Aliveness detection for iris biometrics," *in Proc. 40th Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, pp. 122-129, 2006.

[13] M. Kanematsu, H. Takano, and K. Nakamura, "Highly reliable liveness detection method for iris recognition," *in Proc. Annu. Conf. SICE*, pp. 361-364, 2007.

[14] Z. Wei, X. Qiu, Z. Sun, and T. Tan, "Counterfeit iris detection based on texture analysis," *in Proc. 19th Int. Conf. Pattern Recognit. (ICPR)*, pp. 1-4, 2008.

[15] K. W. Bowyer and J. S. Doyle, "Cosmetic contact lenses and iris recognition spoofing," *in Computer*, vol. 47, no. 5, pp. 96-98, 2014.

[16] 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," *in IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 851-862, 2014.

[17] N. Kohli, D. Yadav, M. Vatsa, and R. Singh, "Revisiting iris recognition with color cosmetic contact lenses," *in Proc. IAPR Int. Conf. Biometrics (ICB)*, pp. 1-7, 2013.

[18] J. S. Doyle, K. W. Bowyer, and P. J. Flynn, "Variation in accuracy of textured contact lens detection based on sensor and lens pattern,"*in Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS)*, pp. 1-7, 2013.

[19] X. Huang, C. Ti, Q.-Z. Hou, A. Tokuta, and R. Yang, "An experimental study of pupil constriction for liveness detection," *in Proc. IEEE Workshop Appl. Comput. Vis. (WACV)*, pp. 252-258, 2013.

[20] T. Kathikeyan and B. Sabarigiri, "Countermeasures against IRIS spoofing and liveness detection using Electroencephalogram (EEG)," *in Proc. Int. Conf. Comput., Commun., Appl. (ICCA)*, pp. 1-5, 2012.

[21] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," *in Proc. IAPR Int. Conf. Biometrics (ICB)*, pp. 271-276, 2012.

[22] P. Pudil, J. Novovicova, and J. Kittler, "Floating search methods in feature selection," *in Pattern Recognit. Lett.*, vol. 15, no. 11, pp. 1119-1125, 1994.

[23] A. F. Sequeira, J. Murari, and J. S. Cardoso, "Iris liveness detection methods in mobile applications," *in Proc. Int. Conf. Comput. Vis. Theory Appl. (VISAPP)*, pp. 22-33, 2014.

[24] A. F. Sequeira, J. Murari, and J. S. Cardoso, "Iris liveness detection methods in the mobile biometrics scenario," *in Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, pp. 3002-3008, 2014.

[25] J. C. Monteiro, A. F. Sequeira, H. P. Oliveira, and J. S. Cardoso, "Robust iris localisation in challenging scenarios," *in Computer Vision, Imaging and Computer Graphics: Theory and Applications (Communications in Computer and Information Science), Berlin, Germany: Springer-Verlag*, 2004.

[26] Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," *in IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 6, pp. 1120-1133, 2014.
[27] F. Smeraldi, M. Bicego, M. Cristani, and V. Murino. "CLOOSTING: CLustering Data with bOOSTING." *In MCS*, pp. 289-298. 2011.
[28] L. Ghiani et al., "LivDet 2013—Fingerprint liveness detection competition," *in Proc. Int. Conf. Biometrics (ICB)*, pp. 1–6, 2013. [Online]. Available: http://prag.diee.unica.it/fldc/
[29] A. Czajka, "Database of iris printouts and its application: Development of liveness detection method for iris recognition," *in Proc. 18th Int. Conf. Methods Models Autom. Robot. (MMAR)*, pp. 28-33, 2013.
[30] KNIME, Knime Analytics Platform. Available at https://www.knime.com/knime-analytics-platform
[31] N. Mowla, I. Doh, K. Chae, "Selective fuzzy ensemble learner for cognitive detection of bio-identifiable modality spoofing in MCPS", *in 20th International Conference on Advanced Communication Technology (ICACT)*, pp. 63-37, 2018.

Nishat Mowla was born on 1st August, 1989. She received the B.S degree in computer science from Asian University for Women, Chittagong, Bangladesh in 2013, an M.S. degree in computer science and engineering from Ewha Womans University, Seoul, Korea in 2016.

She worked at Asian University for Women, Chittagong, Bangladesh as a Senior Teaching Fellow. She is currently a Ph.D. student at Ewha Womans University, Seoul, Korea. Her research interests include next generation network security, IoT network security and network traffic analysis.

Ms. Mowla received the best thesis award for her Master's thesis in 2016. She was awarded the best paper award in the Qualcomm 2017 paper competition. She also received the outstanding paper award in the 19th International Conference on Advanced Communication Technology (ICACT) in 2017.

Inshil Doh was born on 3rd March, 1970. She received the B.S. and M.S. degrees in computer science and engineering at Ewha Womans University, Korea, in 1993 and 1995, respectively. She received the Ph.D. degree in computer science and engineering from Ewha Womans University in 2007.

She was a research professor of Ewha Womans University in 2009~2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. Her research interests include wireless network, sensor network security, and M2M network security.

From 1995-1998, Prof. Doh worked in Samsung SDS of Korea to develop a marketing system. Prof. Doh received best paper award in Korea information Processing Society in 2009. Prof. Doh also received best paper award in Korea Institute of Information and Communication Engineering Conference in 2015.

Prof. Chae was born on 22nd October, 1957. He received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984. He received a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990.

He is currently a professor in the Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include sensor network, smart grid, CDN, SDN and IoT, network protocol design and performance evaluation.

Prof. Chae was the advisory board member of ACM Transactions on Internet Technology from 2000 to 2004. He was also a member of the International Who's Who from 2001 to 2010.