enhAnced Mobile BiomEtRics

DELIVERABLE: D57 D6.10

AN EAR ANTI-SPOOFING DATABASE WITH VARIOUS ATTACKS

Contract number:	675087
Project acronym:	AMBER
Project title:	Enhanced Mobile Biometrics
Project duration:	1 January 2017 – 31 December 2020
Coordinator:	Richard Guest, University of Kent, Canterbury, UK

Deliverable Number:	D6.10
Type:	Academic Paper 6.6
Dissemination level	PU
Expected submission date	December 2018
Date submitted:	January 2019

Authors / contributors	Jalil Nourmohammadi-Khiarak, Andrzej Pacut
Contributing partners	Warsaw University of Technology

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675087 programme under the Marie Skłodowska-Curie grant

An Ear Anti-spoofing Database With Various Attacks

Jalil Nourmohammadi-Khiarak
Faculty of Electronics and Information Technology
Warsaw University of Technology
Warsaw, Poland
Jalil.Nourmohammadi@elka.pw.edu.pl

Andrzej Pacut
Faculty of Electronics and Information Technology
Warsaw University of Technology
Warsaw, Poland
a.pacut@ia.pw.edu.pl

***Abstract*—the Biometrics of the ears have both advantages and disadvantages compared to other physical attributes. The small surface and the relatively simple structure have a controversial effect. In a positive way, these features provide faster processing compared to face detection and make detection easier compared to fingerprints. On the other side, like other biometrics, current ear biometric recognition systems are vulnerable to attacks. A spoofing attack occurs at sensor level and every impostor can masquerade as someone else by altering data, thus, obtaining an illegitimate access. Due to a lack of anti-spoofing databases, that would support this paper, ear fake databases have been built using different mobile phones. In this paper, an ear presentation attack detection database is collected which contains a various range of variations of potential attacks. In particular, the database consists of two main parts, a) AMI dataset which has 700 ear images and we make display attack by using them, b) data collected at University of Tabriz containing 20 genuine subjects and fake ears which are made from the genuine ears. Different mobile phones are used for collecting the database. Three fake ear attacks are implemented which include video attack, printed attack, and display attack. Consequently, for each subject, 2 videos (left and right ears), 8 different images, and the final database contain 10 video clips and 160 images are prepared. General Image Quality Assessment is used as a baseline algorithm for comparison which is used vastly in the liveness detection purpose. Releasing the first database in ear liveness detection can open new ways for investigating on ear biometrics systems more confidently to use future research on mobile smartphones.**

Keywords— ear recognition systems, spoofing attack, Image Quality Assessment, liveness detection.

I. Introduction

In spite of the fact that ear recognition systems have attained during the past decade [1-5], no effort has been made to make sure how it would work if imposters try to fool the system in mobile device applications. Unaccredited impostors try to find a way to access illegally by showing fake ear to the system. Without having presentation attack detection methods on the recognition systems, they will be successful and steal more vital information on a mobile device.

Ear, similar to a face, is in danger of spoofing by impostors and they can capture a photo using mobile cameras or digital camera, on the other hand, fake ear can be made easily such as presenting videos on a laptop or printing photos. Replay video, 3D mask, and fake photos (printed and displayed photos) are main concerns of attacks in ear recognition systems, so having a powerful presentation attack detection method has the most important position in ear recognition systems.

However, as is clear, there is no dataset for ear anti-spoofing detection. This reason motivates us to create a comprehensive dataset to use as the standard platform for ear presentation attack detection issue. The dataset contains 20 subjects and we are planning to create photos with various qualities and two videos for a subject (left and right ear). In this scenario, there are three types of precise attack designs. For analyzing the dataset, five scenarios are used. Our dataset (collected at University of Tabriz), which is the first dataset, is for ear anti-spoofing detection. We also present an algorithm to start studying in this part of the research. Printing and showing photos reduce the quality of ear texture, so one of the proofs for liveness is the high-frequency information. Complexity degree of the proposed method is lower than 0.1 second, so it is suitable for real-time applications, using 11 general image quality assessment features extracted from one image to distinguish between impostor and legitimate samples. Then we apply an SVM classification function to distinguish between fake and genuine.

II. Data collection

Having a dataset for doing research on all of the issues is the most important challenge, so in this section, the collected anti-spoofing dataset for ear images is illustrated.

The input sensors in an ear recognition system are image cameras; they can use single or multiple photos or videos for protection mechanism. Five different mobiles are used to capture the data with the same qualities. The quality of images is 2448 by 3264 for height and width, respectively. In video parts of the database, using high-quality video

978-1-5386-7931-9/18/$31.00 ©2018 European Union

needs high computational cost so we considered 1920 by 1080 for width and height, respectively. Fig. 1 shows a proposed setup of ear recognition system by a mobile device. Two samples of the data are shown in Fig. 2 which the left one and the right one are related to image and video, respectively.

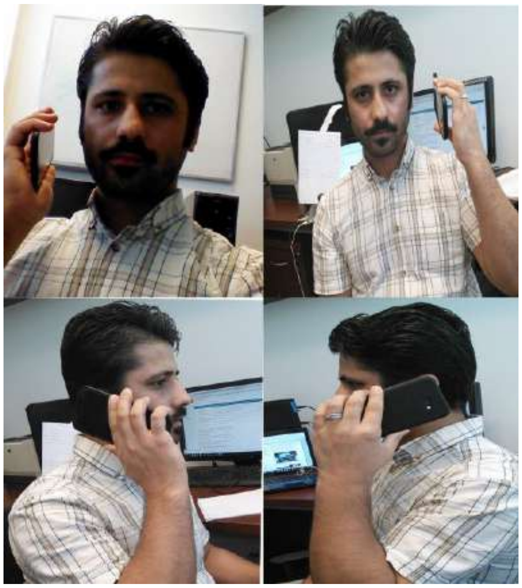

Fig. 1. Process of taking photo of ears.

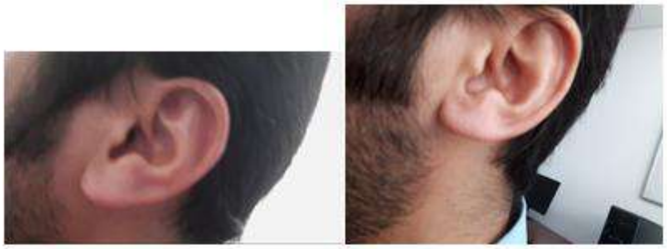

Fig. 2. Video and photo of ear images. The left one is video sample and the right one is photo sample of real mages

A. UoT Real Ear Databases

The collected images and videos from the real ears are from 20 subjects. The condition of capturing was completely natural. It means that no brightness or light was added. In image collection, we supposed that this dataset is going to be utilized in mobile applications, so the mobile cameras were beside the ear with 15 centimeters. For each subject, 8 images were taken which are shown in detail in Table I.

A Samsung Galaxy A7, an iPhone 6s, a Samsung Galaxy 7 Edge, and other mobile devices are used to capture images. Six of the captured images are right ear which is divided two parts, three from front camera, and three from the rear camera. The rest six images are captured from left ear similar the right ear. Two videos are captured from both left and right ears during six to ten seconds. Totally, the databases of 160 images and 10 videos have been recorded. Fig. 3 shows an instance of the database.

TABLE I. DETAIL OF NUMBER OF EAR IMAGES (ER) AND VIDEOS ARE CAPTURED USING MOBILE DEVICES

Back camera		Front camera	
Left ER	Right ER	Left ER Video	Right ER Video
2	2	2 1	2 1

An important aspect of data acquisition is an environmental condition; pose and illumination conditions which can be effective on data. Based on the information, three kinds of attacks can be performed on ear recognition system in a mobile device, which all of them are described in the next part.

B. UoT Fake Ear Databases

Fake ears are the most important part of our dataset. We design our fake ear dataset is based on three types of attacks. We create fake ear using two kinds of ear data, the first one belongs to AMI Ear Database and the second one is our dataset which is described in the previous section. Before discussing the database, we describe the possible attacks on the ear recognition.

Photo attack: Showing an ear photo by attackers to the camera in a mobile device [6], which has ear recognition system, is a photo attack. Based on other biometrics, this kind of attacks can spoof the sensors on recognition systems. Obtaining fake ear photo is easy and it shows that ear biometrics is vulnerable and photo attack should be considered an important issue in presentation attack detection. First, we print the entire genuine photos on A3 glossy paper. For doing so, we used a Canon imagePRESS C6011 printer which had good quality (1200 dpi by 1200 dpi resolution and 256 gradations) and is suitable for making fake images. Then a Samsung Galaxy A7 smartphone camera was used for taking photos of the printed images. The average distance for printed photos is 15 centimeters. The sizes of printed photos are the same size as the genuine ear photo. Fig. 5 shows instance images of spoof and real ears of one subject in our dataset. Our dataset has two advantages: a) all of the images have been captured with the mobile device and they are securely and easily applicable for unlocking phones, and b) the printed photos are generated with a good quality printer and the size of the fake ear is the same size as the genuine ear.

978-1-5386-7931-9/18/$31.00 ©2018 European Union

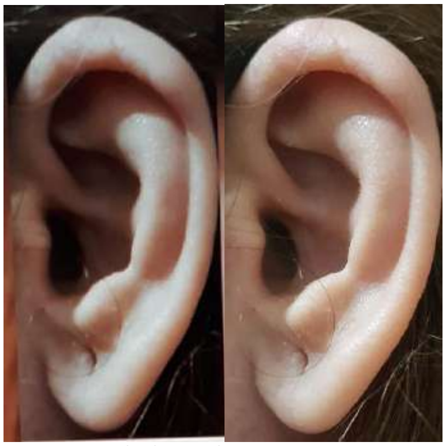

Fig. 3. Example images of a fake (left) and genuine(right) ear of one of the subjects in our database.

Video Attacks: When ear recognition systems use a video of ears in recognition, video attacks appear and like photo attacks, video attack is significant and also it can spoof the system easily [7].

In this case, the listed phones are used for recording the video of subject's ears and a Samsung Galaxy A7 is used for capturing a video which is replayed on the high-resolution device, Samsung Galaxy A7, to generate mobile video attack for ear presentation attack detection. It is noteworthy that the original videos are downsized by the phone screen. The average distance for the mobile video replay is considered like genuine video (~15cm) which is depicted in Fig 4.

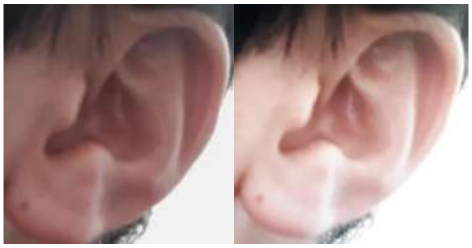

Fig. 4. (left)Genuine ear; (right) Spoof ear are generated using Samsung Galaxy A7 for video replay attack;

Display attack: the attacks are performed using photos taken with the mobile phones [8]. In this case, the photos are displayed using an A ProLite E2208HDS Widescreen LCD screen with resolution 1024 by 768 and it is possible to make ear mask to use for spoofing an ear recognition system.

C. *AMI Ear Database*

Esther Gonzalez collected AMI Ear Database for her Ph.D., 100 subjects are considered in this database and 700 images are taken [9]. The ear photos belong to teachers, students, and staff at Universidad de Las Palmas de Gran Canaria (ULPGC). Nikon D100 camera was used for taking a photo in a certain condition. The dataset is used in several papers [10-13]. Therefore, we make fake photos of this dataset just for display attack purposes [9]. A ProLite E2208HDS Widescreen LCD and a Samsung Galaxy A7 are used for base system and taking photos of showing the image respectively. Fig. 3 shows a sample of fake and genuine ear photos.

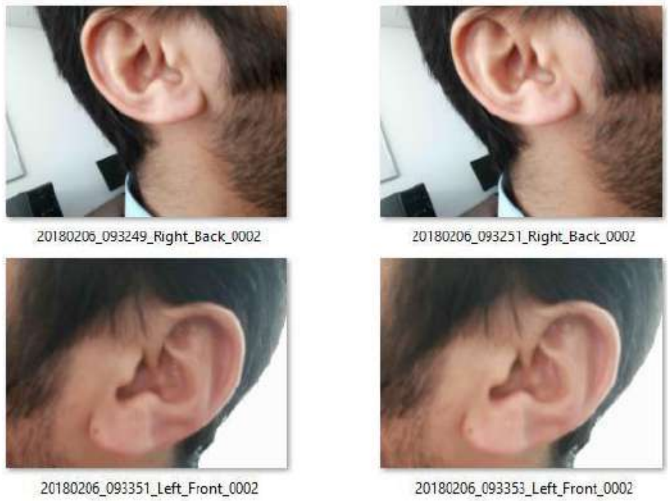
20180206_093249_Right_Back_0002
20180206_093251_Right_Back_0002
20180206_093351_Left_Front_0002
20180206_093353_Left_Front_0002

Fig. 5. An example of images from our real genuine ear dataset

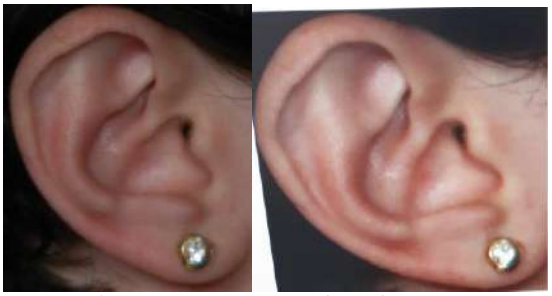

Fig. 6. Real image from AMI dataset in the left and fake image in the right is captured using a mobile camera.

III. TESTING PROTOCOL AND BASELINE METHODS

Having a test protocol and baseline algorithm is necessary for all of the studies about creating database. In this section, we will discuss two important topics; first, the test protocol, second, an algorithm for anti-spoofing detection of ears.

A. *Testing Protocol*

Our database, for the most part, considers various fake ears; five scenarios are designed for the test protocol. We consider the two imaging qualities explicitly (Normal quality test, High-quality test) and the three fake ear attack types (Photo attack, Video Attacks, and Display attack). The data are apportioned into 80% training and 20% test sets.

978-1-5386-7931-9/18/$31.00 ©2018 European Union

IV. Image Quality Assessment(IQA)

In liveness detection, image quality assessment has become confidently proved worthy especially when there is a difference between fake and real images [11-14]. These differences may appear in color and luminance levels, a degree of sharpness, structural distortions, and local artifacts. For example, ear images are captured from a mobile device, will probably be under-exposed or over-exposed because the environmental and input sensors' conditions may differ. In addition, the vast majority of the real images are optical images formed by focusing light onto some sort of 2D sensor arrays through an optical system and by contrast, synthetic images are 2D arrays of data where each array element (pixel) in the 2D array are transformed into color or intensity for display. Both types of real and synthetic are displayed as images, but the difference between real and synthetic are significant. On one hand, the electromagnetic waves struck the array value of the real image from the optical system; on the other hand, some other types of signals are used to compute the array value of the synthetic images.

Image quality for various purposes has been used such as; steganography and image manipulation detection. In addition, image quality has already been used for presentation attack detection purposes in the face, iris, and fingerprint applications.

A. *IQA for liveness detection*

Liveness detection is a two-class classification challenge where an input sample has to be one of two classes: genuine or fake. Finding a better set of discriminant features is the key point in this process which causes to create more precise classification. In this paper, a parameterization using 11 image quality measures is used. The pipeline of the baseline algorithm is depicted in Fig. 7.

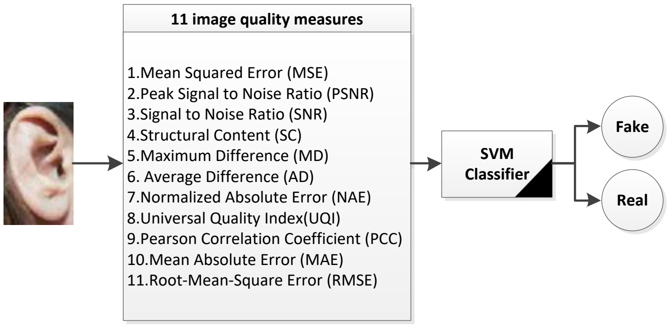
11 image quality measures
1.Mean Squared Error (MSE)
2.Peak Signal to Noise Ratio (PSNR)
3.Signal to Noise Ratio (SNR)
4.Structural Content (SC)
5.Maximum Difference (MD)
6. Average Difference (AD)
7.Normalized Absolute Error (NAE)
8.Universal Quality Index(UQI)
9.Pearson Correlation Coefficient (PCC)
10.Mean Absolute Error (MAE)
11.Root-Mean-Square Error (RMSE)
SVM Classifier
Fake
Real

Fig 7: General diagram of liveness detection method utilizing Image Quality Assessment (IQA)

11-feature parameterizations are used in the present work namely, Mean Squared Error (MSE) [14], Peak Signal to Noise Ratio (PSNR) [15], Signal to Noise Ratio (SNR) [16], Structural Content (SC) [17], Maximum Difference (MD) [17], Average Difference (AD) [17], Normalized Absolute Error (NAE) [18], Universal Quality Index(UQI) [19], Pearson Correlation Coefficient (PCC) [20], Mean Absolute Error (MAE) [17], and Root-Mean-Square Error (RMSE) [21]. The more details about the quality measurements can be found in the related references.

V. Experiment Results & Analysis

In our experimental evaluation, we evaluated multi-attack in ear recognition systems. The method has an ability to make a secure methodology based on liveness detection and prevents fraudulent access. Therefore, in order to reach a suitable result, we created a new database based on two databases namely AMI database and our database. The reason for using AMI database is to show performance of the protocol system in comparison with ear recognition systems without liveness detection. And we created a new fake database to publish and bring a new idea for ear recognitions to research more. As described in IV, the 11-IQM is built with an SVM classifier (see fig 7). So, in all evaluations, we report False Fake Rate (FFR), the probability of false instances which are classified as genuine, and False Real Rate (FRR), the probability of genuine instances which is classified as fake. There is another interesting metric which is called The Half Total Error Rate (HTER) form of FRR and FGR and is HTER = (FFR + FGR)/2.

A. *Fake AMI database*

As we described, AMI database was released [6]. For showing importance of the issue, we made fake databases based on AMI database which is a display attack, which was explained in section II completely. The result of the liveness detection based on baseline algorithm is shown in Table II where it can be seen that the baseline algorithm can classify the samples over 90% correctly. According to the evaluation on training set, all of the HTER were 0, so the baseline algorithm had good results for training set.

TABLE II. RESULTS OF OBTAINED ON THE DISPLAY ATTACK ON TESTING SET OF AMI DATABASE.

Test set	***FFR***	***FRR***	***HTER***
AMI database	0	0	0
Photo attack from UoT	0	3.06	1.53
Display attack from UoT	0	0	0
Video Attacks from UoT	0	0	0

B. *UoT Fake Ear Databases*

This database is made in the University of Tabriz. The details of the database are described in section II. Fig. 3 shows real and fake samples of the database that the fake image is very similar to real images making them suitable for the attacking scenarios. According to the section II, in our database, we have three kinds of attacks which are the results of each of them are shown in Table III. In spite of the fact that the fake and real images are very similar to each other, the overall error of the baseline algorithm is 2.1%.

The interesting part of the results is when various data is used for training and testing goal. The described result at Table III is related to test set (20% of all dataset). It comes to the view that, using the high-quality camera for collecting data has an effect on the results.

TABLE III. RESULTS OF OBTAINED ON TESTSET OUR DATABASE, THE VALUES SHOW HTER.

Test Training	*Photo attack*	*Video attack*	*Display attack*	*All*
Photo attack	1.9	50.18	5.65	21.34
Video attack	1.68	0	2.25	8.86
Display attack	12.5	0.30	1.91	8.52
All	2.1	0.48	5.76	22.4

VI. Conclusion

In this paper, we described an ear anti-spoofing database with various attacks to come as a base database in the literature. The database has 20 genuine subjects, and the fake ears are collected with the various qualities of mobile devices from the genuine ears. Different qualities and three kinds of fake ear attacks are considered as well. A test protocol is designed containing five scenarios for providing an environment to the analysis of factors that impact on the anti-spoofing accuracy. We use an IQA+SVM baseline algorithm to classify genuine and fake ears. To our knowledge, there is no anti-spoofing database for ear recognition systems and the created database can be a starting point for doing other researches in this field.

ACKNOWLEDGMENTS

This project has received funding from the European Union’s Horizon 2020 research and innovation programmed under the Marie Skłodowska-Curie grant agreement No 675087. It would be a great pleasure to the author to thank Mr. Reza Davtalab who helped the authors to collect the database of ear images used in this paper at University of Tabriz-Iran.

REFERENCES

[1] A. S. Anwar, K. K. A. Ghany, and H. Elmahdy, "Human ear recognition using geometrical features extraction," *Procedia Computer Science*, vol. 65, pp. 529-537, 2015.

[2] J. Bhardwaj and R. Sharma, "Ear Recognition Using Self-adaptive Wavelet with Neural Network Classifier," in *Data Engineering and Intelligent Computing*: Springer, 2018, pp. 51-65.

[3] Ž. Emeršič, V. Štruc, and P. Peer, "Ear recognition: More than a survey," *Neurocomputing*, vol. 255, pp. 26-39, 2017.

[4] D. J. Hurley, B. Arbab-Zavar, and M. S. Nixon, "The ear as a biometric," in *Handbook of biometrics*: Springer, 2008, pp. 131-150.

[5] I. Omara, X. Li, G. Xiao, K. Adil, and W. Zuo, "Discriminative Local Feature Fusion for Ear Recognition Problem," in *Proceedings of the 2018 8th International Conference on Bioscience, Biochemistry and Bioinformatics*, 2018, pp. 139-145: ACM.

[6] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in *Biometrics (IJCB), 2011 international joint conference on*, 2011, pp. 1-7: IEEE.

[7] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *Biometrics (ICB), 2012 5th IAPR international conference on*, 2012, pp. 26-31: IEEE.

[8] A. Anjos, M. M. Chakka, and S. J. I. b. Marcel, "Motion-based counter-measures to photo attacks in face recognition," vol. 3, no. 3, pp. 147-158, 2013.

[9] L. A. a. L. M. Esther Gonzalez, "AMI Ear Database, http://www.ctim.es/research_works/ami_ear_database/," *CTIM. Centro de I+D de Tecnologias de la Imagen*
Universidad de Las Palmas de G.C.

[10] K. Annapurani, M. Sadiq, and C. Malathy, "Fusion of shape of the ear and tragus–a unique feature extraction method for ear authentication system," *Expert Systems with Applications*, vol. 42, no. 1, pp. 649-656, 2015.

[11] D. Narayan and S. Dubey, "A Survey Paper on Human Identification using Ear Biometrics," *International Journal of Innovative Science and Modern Engineering (IJISME)*, vol. 2, no. 10, pp. 9-13, 2014.

[12] A. Nikolov, V. Cantoni, D. Dimov, A. Abate, and S. Ricciardi, "Multi-model ear database for biometric applications," in *Innovative Approaches*

978-1-5386-7931-9/18/$31.00 ©2018 European Union

and Solutions in Advanced Intelligent Systems: Springer, 2016, pp. 169-187.

[13] Q. ul Ain, "Multimodal Biometric Security using Evolutionary Computation," Department of Computer Science & Software Engineering for the Partial Fulfillment of the Requirement of MS (CS) Degree By Qurrat ul Ain 639-FBAS/MSCS/F10 Supervised by Dr. Ayyaz Hussain Department of Computer Science and Software Engineering, Faculty of Basic and Applied Sciences, International Islamic University, Islamabad, 2013.

[14] M. Mathieu, C. Couprie, and Y. LeCun, "Deep multi-scale video prediction beyond mean square error," *arXiv preprint arXiv:1511.05440,* 2015.

[15] D. Poobathy and R. M. Chezian, "Edge detection operators: Peak signal to noise ratio based comparison," *International Journal of Image, Graphics and signal processing,* vol. 6, no. 10, p. 55, 2014.

[16] M.-J. Sun, M. P. Edgar, D. B. Phillips, G. M. Gibson, and M. J. Padgett, "Improving the signal-to-noise ratio of single-pixel imaging using digital microscanning," *Optics express,* vol. 24, no. 10, pp. 10476-10485, 2016.

[17] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE transactions on image processing,* vol. 23, no. 2, pp. 710-724, 2014.

[18] M. Khare, R. K. Srivastava, and A. Khare, "Moving object segmentation in Daubechies complex wavelet domain," *Signal, Image and Video Processing,* vol. 9, no. 3, pp. 635-650, 2015.

[19] P. Hanhart, M. V. Bernardo, P. Korshunov, M. Pereira, A. M. Pinheiro, and T. Ebrahimi, "HDR image compression: a new challenge for objective quality metrics," in *Quality of Multimedia Experience (QoMEX), 2014 Sixth International Workshop on*, 2014, pp. 159-164: IEEE.

[20] H. Zhou, Z. Deng, Y. Xia, and M. Fu, "A new sampling method in particle filter based on Pearson correlation coefficient," *Neurocomputing,* vol. 216, pp. 208-215, 2016.

[21] T. Chai and R. R. Draxler, "Root mean square error (RMSE) or mean absolute error (MAE)?– Arguments against avoiding RMSE in the literature," *Geoscientific model development,* vol. 7, no. 3, pp. 1247-1250, 2014.