Efficient Spoofing Attack Detection against Unknown Sample using End-to-End Anomaly Detection

Tetsushi Ohki* and Vishu Gupta* and Masakatsu Nishigaki*
* Shizuoka University, Shizuoka, Japan
E-mail: ohki@inf.shizuoka.ac.jp Tel/Fax: +81-53-478-1471

***Abstract*—With the evolution of a high precision sensor, printing machine, and manufacturing machine, spoofing attacks become a significant threat to the biometric systems. In order to mitigate the threats of diverse and unexpected attacks, conventional spoofing attack detection methods which aim to detect a specific attack are not sufficient. In this study, we propose a end-to-end machine learning technique which can model biometric information with the complicated structure of high dimension by a probability distribution. The proposed system can recognize whether inputted sample is spoofing one or not even if it is an unknown attack.**

I. Introduction

Biometric system registers biometric information collected in advance as a template and confirms the identity by calculating similarity with the biometric information acquired at the time of authentication. As compared to the authentication method using password or token, biometric authentication, which uses the biometric traits of the person is less likely to get stolen or be forgotten by us. In addition to the progress in practical use by this new form of authentication is used in the fields of immigration control, bank ATM, building entrance and exit control, in recent years, the use for more personal applications such as loading on mobile terminals is also spreading. On the other hand, there is a problem that biometric information such as the face, voice, fingerprint, and handwriting is difficult to conceal in daily life. In recent years, the accuracy of the manufacturing of fake biometric information is approaching the real thing with the sensor, the printing machine, and the manufacturing machine which has become highly accurate, and "presentation attacks (a.k.a presentation attacks)" using them is becoming a social threat.

In this paper, we introduce the idea of novel presentation attack detection (PAD) method utilizing unsupervised anomaly detection. While existing methods based on binary classification have to construct a classifier for each type of fake samples, the proposed method can detect unknown samples that are not included in the training data using a single classifier.

Active research on presentation attack detection for biometric devices has been carried out[15], [3], [28], [21], which shows that this presentation attack detection is generally performed independently of the biometric verification process. The authentication sensor extracts biometric characteristics and reactions such as three-dimensionality of the human body and electrical conductivity of the living body (referred to as PAD characteristics) and evaluates the similarity with the previously learned PAD features to determine whether it is a presentation attack. While these methods identify presentation attacks with high accuracy, we require prior knowledge of what kind of artefact the attacker used to perform presentation attacks.

However, high-precision sensors, presentation attack artefacts created by printing machines or manufacturing machines have diversified their attack types, and it has become challenging to learn PAD features that allow the defender to detect all these attacks in advance. Furthermore, by performing anomalous input that is not a biometric sample, the existence of a wolf input capable of impersonating a large number of registered users[14] or arbitrary commands capable of attacking the dialogue speakers(Google, Amazon, etc.) using the inaudible area of the sound[27] etc. has become possible. It is impossible to take measures against these attacks by unknown samples by using the existing method as they are beyond the framework of assumed biometric features.

For such problems, instead of following conventional method where we assume a specific attack and develop a countermeasure against it, we need to innovate the method to counter presentation attack by unknown samples without any prior knowledge on any specific kind of presentation attack.

Unlike the conventional classifier based on binary classification, our proposed presentation attack detection method generates a generative model that defines biometric information model from a large number of biometric information. This model can guarantee the security of the system against the presentation attack as when this biometric information model is compared with input, it classifies the input with low similarity as presentation attack. This makes it possible to fundamentally solve the problem of difficulty in training of PAD features and difficulty to deal with unknown samples simultaneously.

By evaluating the performance of this method using palm image database, we confirmed that it is possible to speed up the process for about 30 times and reduce the data size to about 6% while achieving the same accuracy as the conventional method while performing PAD. The major contributions of this paper are as follows:

- (Section 3) We proposed an presentation attack detection method using an anomaly detection neural network.

- (Section 4) We conducted a performance and an utility evaluation of the proposed method using palm images and showed that the proposed method can detect unknown samples with high accuracy and speed.

II. Related Work

The methods of spoof detection are roughly classified into three major categories. The first category is based on the quality measurement of the image itself. Method for detecting printed material based on two-dimensional Fourier transform [12], method for detecting a living body by modeling the relationship between human retina pattern and light reflection (Lambert reflection) [23], Method using both power spectrum and LBP of an image to utilize texture information and frequency space information [10], etc. are classified into this category. The second category uses the method to distinguish between a spoof attack and a real input by reading various human vital signs. Method to confirm the presence living body where the system requests the user to perform blink at any timing [16], method that incorporates texture information of background area in addition to the blinking of the eyes to perform spoofing detection [17], methods for detecting blinking and mouth movements in a video using dynamic mode decomposition [24], etc. are classified into this category. The final category is a method that focuses on the difference between human and presentation attacks. Many of these presentation attacks are premised on the occurrence of unnatural motions which are different from that of the human body, such as flat motions in printed material. Typically, the determination is performed based on a motion vector detected using optical flow [5]. Also, a method to detect presentation attack by measuring the displacement of time-series texture information [6] which uses the difference in movement between the full view (face) and the background by optical flow[2] are classified into this category. These existing methods detect presentation attacks by applying features such as LBP and optical flow calculated from the input information by a classifier.

On the other hand, in recent years, methods using CNN have outperformed other methods, particularly in computer vision tasks [11], [22]. From this, there has been many researches that proposed the usage of CNN in presentation attack detection. Method using CNN to perform anomaly detection by considering image quality and motion from video [8], method using LSTM-CNN to calculate anomaly score by integrating multiple video frames [26], method using multitasking CNN integrating depth information and face patch information to detect spoofing [4], etc. are example of some of the researches that has been done using CNN technique.

Here, from the information necessary for training, it can be said that all of the above existing methods are algorithms that perform two-class classification using real and fake sample. Therefore, it is necessary to prepare a large number of real and fake sample for training. In addition to the collection of the real sample for the creation of the fake sample, the production process of the fake sample is added, so it often takes time and cost to generate a large amount of fake sample as compared with the collection of the real sample only. Since the biometric detection algorithm using anomaly detection discussed in this paper uses only the real sample as a training sample, we do not have to collect and use a fake sample for the process of the training model. There is a method that enables anomaly detection by integrating multiple features, including PAD features obtained from a single real sample to perform similarity examination, but it considers the similarity of the information, i.e., it uses matching score to perform anomaly detection. This method may be considered sufficient to perform anomaly detection, but this process is challenging to apply when it is used for tasks such as registration and identification. In this paper, we propose a method to perform presentation attack detection precisely from a single matching image that can be used for registration and identification tasks by applying CNN-based anomaly detection algorithm.

A. Anomaly Detection Neural Network

Most of the anomaly detection algorithms using neural networks are based on the theory of generative neural networks model such as Generative Adversarial Networks (GAN) and autoencoder. For example, AnoGAN [20] is an anomaly detection algorithm using GAN. It uses DCGAN with generative model G which learns the mapping of image space $x \in \mathcal{X}$ from latent variable $z \in \mathcal{Z}$ and search for the latent variable z corresponding to the normal image x under the assumption that there is an instance $G(z)$ on the generaitve model which can approximate x. Thus, the problem of anomaly detection in neural networks using generative models can be reduced to the problem of finding the mapping from input image x to latent space $\mathcal{Z}$. For this problem, in addition to the process of searching on the latent space using error back propagation like AnoGAN, a method with the function $E(\cdot)$ to learn the mapping not only for z to x but also from x to z has been proposed in order to make the searching efficient [7]. On the other hand, in all existing methods using GAN, as a part of the network used for training is deleted and is utilized for anomaly value detection such as the training network and the identification network are different which makes it necessary for the network to re-learn the identification network. To solve this problem, an end-to-end type anomaly detection neural network called ALOCC, which is a combination of Denoising Autoencoder [25] and CNN has been proposed [19]. ALOCC learns both the mapping from x to z and z to x by using autoencoder, and combines this with CNN make it possible to perform anomaly detection using End-To-End network. In this paper, we propose a biometric spoofing detection using ALOCC, and compare it with the existing method which uses anomaly detection algorithms such as AnoGAN and 1-class SVM.

III. Unsupervised presentation attack Detection

In this section, we explain the method for detecting presentation attacks on biometric authentication devices.

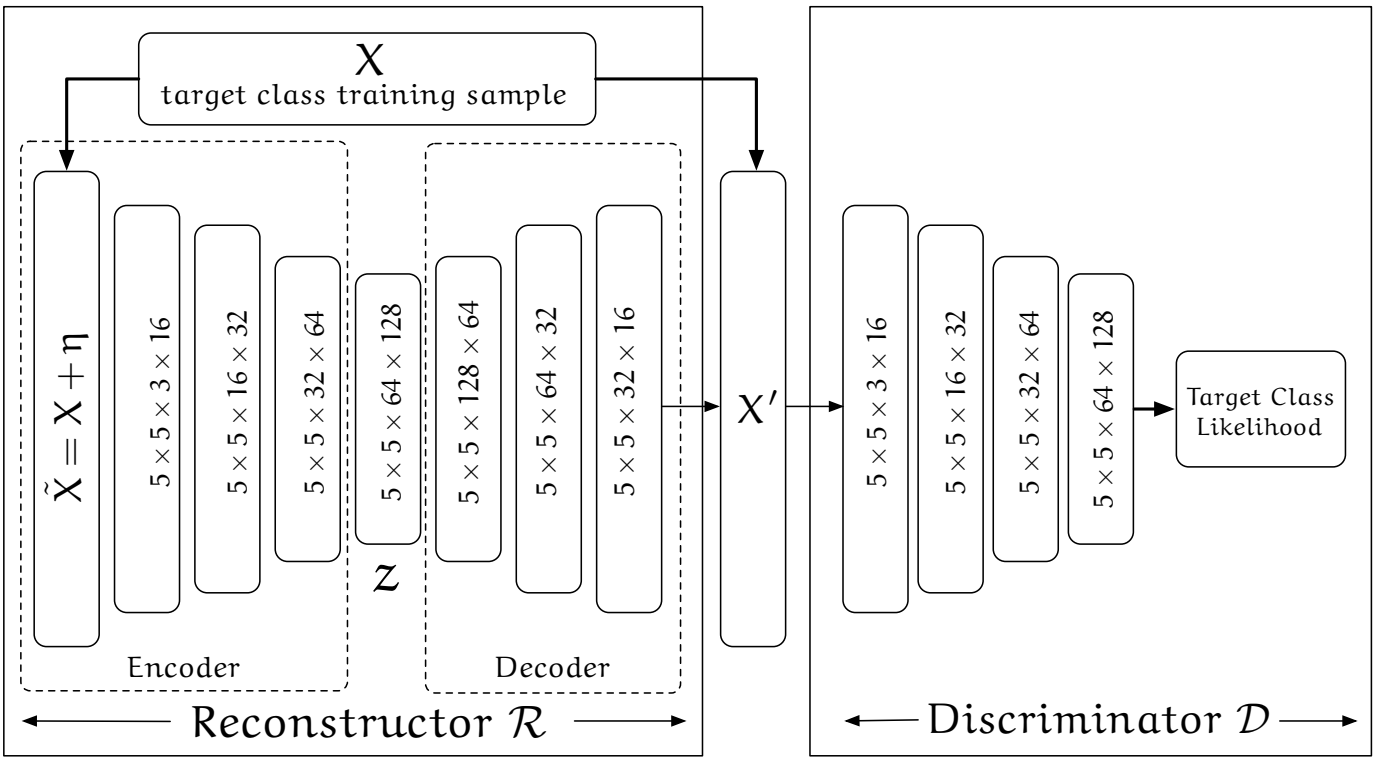


Fig. 1: Architecture of our ALOCC

A. *Adversarially Learned One-Class Classifier*

Our anomaly detection based presentation attack detection is based on Adversarially Learned One-Class Classifier for Novelty Detection (ALOCC) proposed in [19].

The network configuration of ALOCC used in this paper is shown in Fig. 1. The Reconstructer module $\mathcal{R}$ in ALOCC is configured by Denoising Autoencoder [25] (known as DAE). DAE is one of the methods used in unsupervised neural network which calculate an image $\tilde{X} = X + \eta$ from input X with adding the noise η to an input image X to destroy a part of the image. The network trains a function $\mathcal{R}$ to restore the image X from the image with noise $\tilde{X}$ (Note that we can use Gaussian noise, Salt and Pepper, etc. as noise sources). To improve the discrimination performance of this method, ALOCC input the original image X and reconstructed image X' to the seconde module, called discriminator $\mathcal{D}$. Discriminator $\mathcal{D}$ is assumed that the reconstructor $\mathcal{R}$ is trained by the normal image and the difference between X' and X for normal images is more smaller than that of anomaly images.

In [19], they used the Denoising Autoencoder with the middle layer as $5 \times 5 \times 256 \times 512$. In this paper, we reduced the number of parameters by making it $5 \times 5 \times 64 \times 128$. The network $\mathcal{R} + \mathcal{D}$ which is a combination of $\mathcal{R}$ and $\mathcal{D}$ has the same architecture like that of the Generative Adversarial Nets(GAN)[9] proposed by the Goodfellow, and it can also be learned in the same method of Generative Adversarial Network. GAN is an algorithm that aims at generating samples that follow the same distribution as training data through generative adversarial training of the two networks Generator G and Discriminator D. G learns the function G by sampling an arbitrary random vector z from the latent space $\mathcal{Z}$ represented by the distribution p_z and maps it to the actual data distribution p_t whereas D aims to distinguish between training data and generated data produced by G. Generator and Discriminator performers advance training by where both the network perform min-max game which is represented by the following equation:

$$\min_G \max_D (\mathbb{E}_{X \sim p_t}[\log D(X)] + \mathbb{E}_{Z \sim p_z}[\log(1 - D(G(Z)))]) \quad (1)$$

On the other hand, in ALOCC, instead of mapping the vector on the latent space $\mathcal{Z}$ to the sample on the distribution p_t, it learns the mapping from the noise added image $\tilde{X}$ to the normal image using DAE. Assuming that the normal distribution of the noise added to the image is $N_\sigma = \mathcal{N}(0, \sigma^2, \mathrm{I})$ the following formula represents the min-max game in ALOCC:

$$\min_{\mathcal{R}} \max_{\mathcal{D}} (\mathbb{E}_{X \sim p_t}[\log \mathcal{D}(X)] + \mathbb{E}_{\tilde{X} \sim p_t + N_\sigma}[\log(1 - \mathcal{D}(\mathcal{R}(\tilde{X})))]) \quad (2)$$

Also, as for the loss function $\mathcal{L}_{\mathcal{R}+\mathcal{D}}$ used for training, we use the loss function of the combined network $\mathcal{R} + \mathcal{D}$. In addition to this, to effeiciently perform the training for the latent space, we take into consideration the loss $\mathcal{L}_{\mathcal{R}}$ on the output of R during the training process which is as follows:

$$\mathcal{L}_{\mathcal{R}} = ||X' - X|| \quad (3)$$

Thus, the model is optimized to minimize the final loss function $\mathcal{L}$ which is a linear combination of $\mathcal{L}_{\mathcal{R}+\mathcal{D}}$ and $\mathcal{L}_{\mathcal{R}}$ which is given as follows:

$$\mathcal{L} = \mathcal{L}_{\mathcal{R}+\mathcal{D}} + \lambda \mathcal{L}_{\mathcal{R}} \tag{4}$$

B. Pre-Processing

[19] performs the evaluation experiments related to anomaly detection for major open databases such as MNIST and Caltech256, but in this paper, we conduct an experiment using ALOCC where live palm images do the training, and then we evaluate the performance of anomaly detection with test samples containing fake samples. Since the image resolution differs for MNIST, Caltech256, and palm images, we converted the resolution to 56×80 pixels before giving the image as an input. As this paper aims at end-to-end anomaly detection that does not depend on any existing pre-processing algorithm, the network was given those images as an input which was taken with the camera with only its resolution changes. Here, we didnt perform any pre-processing such as extraction of background area or extraction of ROI (Region of Interest) which is widely used in palm print authentication.

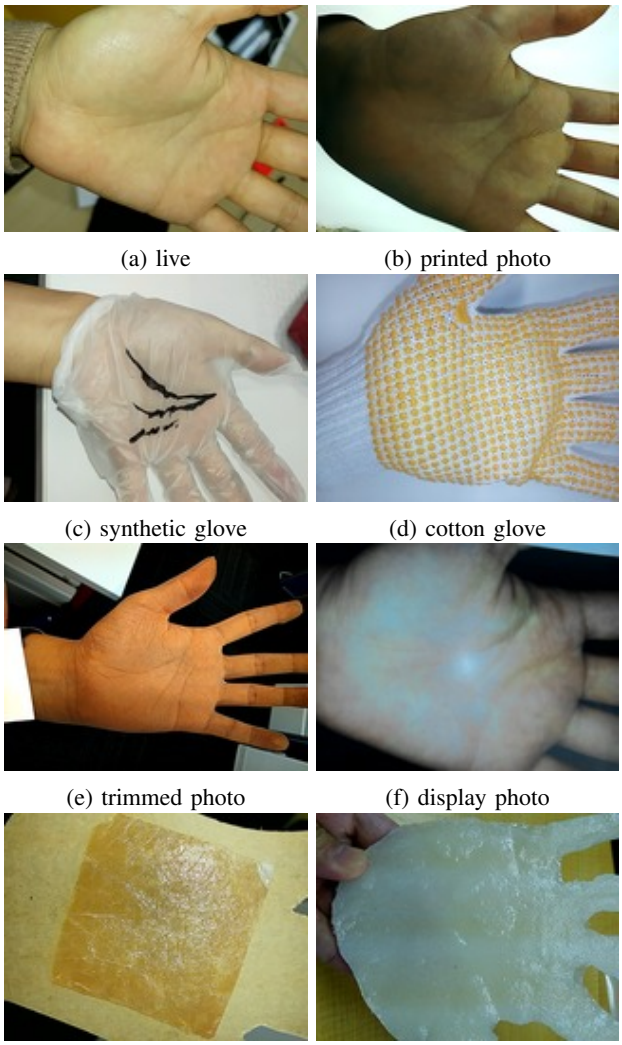
IV. Experiment

The purpose of the experiment is to evaluate the effectiveness of presentation attack detection by using palm images by the proposed anomaly detection network. Therefore, several evaluation methods such as evaluation of detection probability of presentation attack, evaluation of detection speed compared with existing methods, comparison of model size, etc., have been taken into consideration to show that the proposed method is an effective in terms of performance as well as practical use.

A. Database

Many previous works have used public live/fake dataset such as Replay-Attack Database[3] and Unconstrained Smartphone Spoof Attack (USSA) Database[18]. However, it contains only a specific type of fake photo and video samples making it inadequate in terms of anomaly samples. Therefore, in our experiment, we constructed a custom-made database to make sure that the system is being able to make a clear distinction between live and fake samples even when the system encounters unexpected inputs such as palm with a glove, palm with a vinyl glove, etc. which have no direct relation with the hand. Therefore, in our custom-made database, we prepared a large amount of data to evaluate whether the system will be robust to counter various unknown samples.

The custom-made database used in the experiment consists of 8748 live samples and 6648 fake samples of palm with an image resolution of 1280×720 pixels taken directly from approximately 2000 people with ten different types of mobile cameras (LG G5, LG Nexus 5x, LG Nexus 5, Sony Xperia X Performance, Elephone P9000, Sharp Aquos SHV34, Doogee X5max, Huawei GR5 (KII-L22), ASUS zenfone2 (Z00D), ASUS P008). The images are taken in different non-controlled indoor surrounding conditions such as, inside office with different background or inside the building with varying conditions of lighting which also includes photo that is made in a dark place with the help of flashlight, etc. with varying postures in order to anticipate all kind of possibilities of the images that will be used as the input for the system. The training set used to train the model comprises of randomly selected 8000 live samples. The test set in total consists of 7396 samples out of which 748 were live palm samples and 6648 were fake palm samples from cases not included in the training set. The training that we are performing in this experiment is uncontrolled without of external interference. Example of true samples and different variety of fake samples that were used while training the system is given as below in Fig. 2. In order to include as many variety of unexpected fake samples as possible to check the accuracy of the system, we included photos such as (b)printed photo, (c)hand wearing synthetic glove, (d)hand wearing cotton glove,(e)printed photo



(a) live (b) printed photo (c) synthetic glove (d) cotton glove (e) trimmed photo (f) display photo (g) ham (h) synthetic compound

Fig. 2: Examples of samples used for training and testing: (a) is a live sample used for training, and (b) through (h) are various types of fake samples used for testing.

that were cut from the border of the hand part in order to resemble hand in 2D, (h)gelatin or (g)ham which may not have direct relation with the hand but can resemble skin and (f)photo that were taken from a digital device such as iPad or webcam.

B. Evaluation Protocol

The training process in end-to-end anomaly detection network using ALOCC is performed using only live samples to create a model comprised of features from those samples. For this purpose, we selected 8,000 live samples from the palm image database and performed the training of the network. Also, randomly selected 100 fake samples and 100 live samples which are not included in the training samples were used for the testing purpose. The experiment was performed by keeping the loss ratio λ of the loss function $\mathcal{L}_{\mathcal{R}+\mathcal{D}}$ and $\mathcal{L}_{\mathcal{R}}$ as 0.2. To show the effectiveness of the proposed method, 1-Class SVM [13] which is a typical anomaly detection method, and another neural network based anomaly detection algorithm which is called AnoGAN[20] was selected as the method of comparison. All of the methods used in this experiment used the same number of training samples and testing samples for the evaluation process. We used histogram of uniform Local binary pattern (LBP) with a radius of 2 pixels and points of 16 as the feature of 1-Class SVM. Also, the RBF kernel was selected as the 1-Class SVM, and evaluation was performed while changing the value of ν, which determines the rate of anomaly data in the training data from 0 to 1. In AnoGAN, as mentioned in the results of [20], we set the number of backpropagation steps α to 100 to search the latent space using input image. In addition, we used residual score as metric for differentiating live samples and anomaly samples.

In Table I, we show the relation between the input and output for the presentation attack detection system and the general evaluation protocol for data classification such as True Positive, True Negative, False Positive, and False Negative. Also, Area Under Curve (AUC) and Receiver Operation Characteristic Curve (ROC curve) are used as the evaluation protocols for our experiment. In addition to this, we evaluate the result with Half Total Error Rate (HTER), which is often used as a method of evaluation for presentation attack detection algorithm of biometric authentication. The ROC curve has False Positive on the horizontal axis and True Positive on the vertical axis, and the relationship between the two is represented as a curve. The AUC represents the area under the ROC curve and is an index indicating the performance of the classification algorithm. The calculation of HTER is done in a way that the sum of True Negative and False Positive is the smallest, which can be obtained as $\min(TN + FP)/2$.

C. Evaluation Results

1) Evaluation of the Performance for presentation attack Detection: Figure 3 shows the ROC curve, which is the results of the presentation attack detection performance by 1-Class SVM, AnoGAN, and ALOCC. It can see from Table II that the method using each ALOCC significantly outperforms the

TABLE I: Input-output data and evaluation index in presentation attack detection system (TP:True Positive / TN: True Negative / FP: False Positive / FN: False Negative)

		Output	
		Live	Fake
Input	Live	TP	TN
	Fake	FP	FN

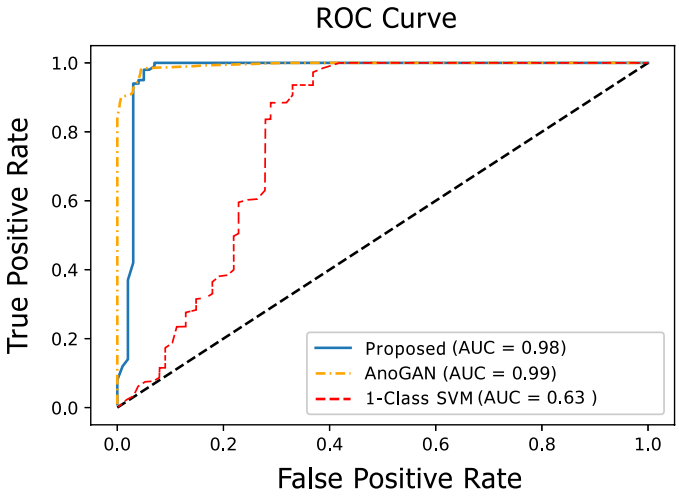


Fig. 3: Experimental results (ROC curve). The dashed diagonal line indicate equal error rates when TP = FP.

method using 1-Class SVM in presentation attack detection performance. Also, as compared to AnoGAN, it has achieved almost the same presentation attack detection performance for AUC and HTER.

2) Evaluation for Usefulness: In Table III, we show the execution time per the decision of 1-Class SVM, AnoGAN, and the proposed method. The execution time was measured with Intel(R) Corei7(R) CPU 5930K a 3.50 GHz CPU and NVIDIA(R) GeForce GTX 1080 Ti GPU. In terms of execution time, the 1-Class SVM overwhelmed the others. On the other hand, it is clear that, due to the nature of the method of backpropagation on latent space, AnoGAN takes a very long time per decision. It can be said that the execution time can be speeded up by reducing or stopping the backpropagation midway by reducing the number of backpropagation α, which is the maximum number of backpropagation, but the number of backpropagation has a trade-off relationship with classification performance. Therefore, practically it is difficult to think about setting the number of backpropagation to a too small value. On the other hand, it is clear that the execution time can be significantly reduced compared with AnoGAN since the proposed method makes use of the Autoencoder, which does not require backpropagation on the latent space. We also compared the number of parameters which indicates the size of the network using a neural network for AnoGAN and the proposed method, as shown in Table IV. It can be seen that for our proposed method, the number of parameters can be reduced to about 6% while maintaining the same presentation attack detection performance as AnoGAN.

TABLE II: Comparison of AUC and HTER

Method	AUC	HTER
1-Class SVM	0.63	0.28
AnoGAN	0.97	0.03
Proposed	0.98	0.04

TABLE III: Execution time per decision

Method	Execution Time
1-Class SVM	0.2 msec
AnoGAN	4018 msec
Proposed	127 msec

V. Discussion

A. presentation attack scenario for biometric authentication system

The block diagram of the biometric authentication system, including presentation attack detection, consists of presentation attack detection subsystem and authentication subsystem as shown in 4(Here, note that presentation attack is termed as presentation attack in [1]). When the authentication subsystem is available, it is possible to reject the input if the registered template and input do not match even when the PAD subsystem is broken, that is, even if presentation attack detection fails. On the other hand, in scenarios such as the registration process and blacklist matching, the authentication subsystem cannot be used because there are no registered templates.

Among the various threats caused by the registration of unauthorized data is the decrease in the reliability of the entire system by registering false information that easily matches with others, or increases of load to the entire system by registering a large number of users who can not exist in the first place. Also, in the blacklist matching, it is clear that the countermeasure becomes more difficult for the attacker because “penetration of the PAD subsystem by fake sample” is the only condition for a successful attack.

Conventional biometric authentication often involves a supervisor in registration and collation processing, and such a problem has not come to the surface, but in recent years opportunities for remote biometric information registration from mobile terminals, etc. must have increased. In the future, it is expected that there will be more situations where it is necessary to take measures against impersonation to the PAD subsystem with such unknown inputs.

B. Limitations

Since ALOCC is an anomaly detection method based on neural networks, it requires a large amount of training data. Also, since it is an end-to-end type network, it learns the generative model and the discrimination model of the system simultaneously, which requires more training data as compared to the conventional anomaly detection neural network. This is a problem for the training process of the system since the cost of collecting biometric information is generally high. To solve this cost related problem, we may use the transfer training method for training the reconstructor and discriminator with existing well-trained biometric models.

TABLE IV: Number of network parameters

Method	Number of Parameters
AnoGAN	9.6 Million

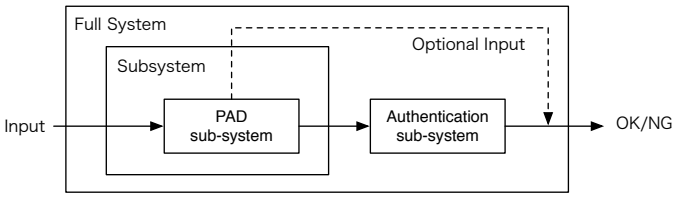


Fig. 4: Diagram showing the configuration of biometric authentication system including presentation attack detection (PAD). PAD-only evaluation is called subsystem evaluation, and the whole evaluation including certification is called full system evaluation [1]

VI. Conclusion

We proposed a spoofing (presentation) attack detection algorithm for biometric authentication using an anomaly detection neural network. The performance of the detection algorithm was evaluated using the database consisting palm image, and the effectiveness was evaluated in terms of calculation time and model size. In the future, with the advancement of manufacturing and image processing technology, the threat of spoofing attack may also diversify and become a severe threat to society. The spoofing attack detection method proposed in this research is a method that enables radical measures against biometric spoofing attacks using only live samples, and we hope that this research to be a trigger for the spread of biometric authentication in the future.

Acknowledgement

We want to thank the president of Normy Corporation Eizaburo Iwata and Hiroki Kamanaka for their assistance and advice in conducting this research. Normy Corporation provided the palm image dataset used in this research. A part of this research is funded by JSPS research grant 18K11294 and 18KT0051.

References

[1] I. J. S. 37. ISO/IEC 30107-3:2017 “Information technology – Biometric presentation attack detection – Part 3: Testing and reporting”, 2017.
[2] A. Anjos, M. M. Chakka, and S. Marcel. Motion-based counter-measures to photo attacks in face recognition. *IET biometrics*, 3(3):147–158, 2013.
[3] 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*, pages 1–7. IEEE, 2011.
[4] Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu. Face anti-spoofing using patch and depth-based CNNs. In *Biometrics (IJCB), 2017 International Joint Conference on*, pages 319–328. IEEE, 2017.
[5] W. Bao, H. Li, N. Li, and W. Jiang. A liveness detection method for face recognition based on optical flow field. In *Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on*, pages 233–236. IEEE, 2009.
[6] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel. LBP-TOP Based Countermeasure against Face Spoofing Attacks. In *Computer Vision-ACCV 2012 Workshops*, pages 121–132. Springer, 2013.

[7] J. Donahue, P. Krähenbühl, and T. Darrell. Adversarial Feature Learning. *arXiv.org*, June 2016.

[8] L. Feng, L.-M. Po, Y. Li, X. Xu, F. Yuan, T. C.-H. Cheung, and K.-W. Cheung. Integration of image quality and motion cues for face anti-spoofing: A neural network approach. *Journal of Visual Communication and Image Representation*, 38:451 – 460, 2016.

[9] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio. Generative adversarial nets. In *Advances in neural information processing systems*, pages 2672–2680, 2014.

[10] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim. Face liveness detection based on texture and frequency analyses. In *Biometrics (ICB), 2012 5th IAPR International Conference on*, pages 67–72. IEEE, 2012.

[11] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In *Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1*, NIPS'12, pages 1097–1105, USA, 2012. Curran Associates Inc.

[12] J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detection based on the analysis of fourier spectra. In *Biometric Technology for Human Identification*, volume 5404, pages 296–304. International Society for Optics and Photonics, 2004.

[13] L. M. Manevitz and M. Yousef. One-class svms for document classification. *Journal of machine Learning research*, 2(Dec):139–154, 2001.

[14] T. Ohki and A. Otsuka. Theoretical vulnerabilities in map speaker adaptation. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2042–2046. IEEE, 2017.

[15] A. Pacut and A. Czajka. Aliveness Detection for IRIS Biometrics. In *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, pages 122–129. IEEE, 2006.

[16] G. Pan, L. Sun, Z. Wu, and S. Lao. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on*, pages 1–8. IEEE, 2007.

[17] G. Pan, L. Sun, Z. Wu, and Y. Wang. Monocular camera-based face liveness detection by combining eyeblink and scene context. *Telecommunication Systems*, 47(3-4):215–225, 2011.

[18] K. Patel, H. Han, and A. Jain. "Secure Face Unlock: Spoof Detection on Smartphones,". June (2016).

[19] M. Sabokrou, M. Khalooei, M. Fathy, and E. Adeli. Adversarially Learned One-Class Classifier for Novelty Detection. In *CVPR*, 2018.

[20] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In *Proceedings of the 25th International Conference of the Information Processing in Medical Imaging IPMI 2017, Boone, NC, USA*, pages 146–157, June 2017.

[21] I. Sluganovic, M. Roeschlin, K. B. Rasmussen, and I. Martinovic. Using Reflexive Eye Movements for Fast Challenge-Response Authentication. In *the 2016 ACM SIGSAC Conference*, pages 1056–1067, New York, New York, USA, 2016. ACM Press.

[22] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. Deepface: Closing the gap to human-level performance in face verification. In *2014 IEEE Conference on Computer Vision and Pattern Recognition*, pages 1701–1708, June 2014.

[23] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In *European Conference on Computer Vision*, pages 504–517. Springer, 2010.

[24] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. Ho. Detection of face spoofing using visual dynamics. *IEEE transactions on information forensics and security*, 10(4):762–777, 2015.

[25] P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol. Extracting and composing robust features with denoising autoencoders. In *ICML*, pages 1096–1103, New York, New York, USA, 2008. ACM Press.

[26] Z. Xu, S. Li, and W. Deng. Learning temporal features using lstm-cnn architecture for face anti-spoofing. In *2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR)*, pages 141–145, Nov 2015.

[27] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 103–117. ACM, 2017.

[28] C. X. Zhao, T. Wysocki, F. Agrafioti, and D. Hatzinakos. Securing handheld devices and fingerprint readers with ECG biometrics. In *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on*, pages 150–155. IEEE, 2012.