SMILE BIOMETRIC IMPRINT CREATION WITH THE USE OF AUTOENCODER

B.A. Assanovich, N.N. Bich, A.F. Pronevich

Non-contact biometric identification and autentification methods with high reliability and security have become very popular in recent years in both social and financial areas. A new biometric imprint was proposed, which is obtained from smile video using stacked autoencoder that allows to build a biometric cryptosystem based on fuzzy commitment [1]. Despite the fact that there are a number of techniques that use facial dynamics to identify a person with the use of various spatio-temporal parameters of face, the deep learning methods are increasingly being exploited for various recognition tasks. Classical linear methods of image processing and feature extraction based on principal components analysis (PCA) are replaced by non-linear transformations. Compared with PCA, the use of an autoencoder significantly increases the classification accuracy, especially with a large number of items [2]. In our setup we applied so-called stacked autoencoder (SAE) that is a neural network including several layers of sparse autoencoders where output of each hidden layer is connected to the input of the successive hidden layer. In this case the hidden layers are trained in an unsupervised way and then fine-tuned by a supervised method.

The use of SAE will allow the use of the trained data of the output layer of the neural network as features for biometric separation of users into genuine and imposters (persons who pretends to be somebody else). The effectiveness of user comparisons depends on similarity rates, which are often determined by the distribution of root mean square (RMS) distances of their characteristics. The more the two distributions are separated and the smaller the standard deviation for each distribution, the better the separation of the classified classes. This property of distributions is estimated by such a parameter as decidability index

Recent research has shown that neural networks like autoencoders have better performance in feature separation compared to PCA technique. Inspired by a possible improvement in the classification characteristics, we used an auto-encoder to obtain biometric data on a person's smile and bind them to a secure user key. Due to the fact that biometric data has instability, error correction codes (ECCs) should be adopted to ensure that fuzziness of biometric data can be alleviated.

According to our knowledge, the use of auto-encoders to create a biometric imprint from face dynamics the context of implementing Biometric Cryptosystem (BC) and linking the secret key to a human smile have not been considered before. We have introduced the term smile-imprint of the user for biometric data Y obtained from the SAE output layer and then used to obtain the personal key with the use of error correcting codes (ECC),

Despite the widespread use of binary BCH codes, recently, interest has grown in non-binary ECC, which also found the application in the creation of Physical Unclonable Function (PUF) for secure storage of cryptographic keys and tamper-detection systems.

Using the designed FaceAnalizer program [3] video was obtained with a person's smile and its three phases: 1.onset (neutral to expressive) phase; 2.apex; and 3.offset phase (expressive to neutral), describing the state of a smiling person's face, were detected and analyzed.

A series of experiments with different dimensions of the intermediate layers were performed with SAE to get good compact biometric features. To reduce time spent, in these experiments the subsets of 40 subjects randomly selected from the entire UvA-NEMO Database were used, reproducing a posed smile. Then normalized grayscale images of from corresponding video of 112x112 pixels in size, scaled to 50%, creating a vector length of the input layer of 0.5x112x112=6272 elements have been used for unsupervised learning of SAE. The results obtained have shown much better performance compared to baseline methods.

References

1. Juels A., Wattenberg M. A fuzzy commitment scheme // Proc. ACM Conf. on Computer and Communications Security. – 1999. – P. 28–36.

2. Mei Wang, Weihong Deng. Deep Face Recognition: A Survey // Computer Vision and Pattern Recognition. – arXiv:1804.06655 https://arxiv.org/abs/1804.06655.

3. Assanovich B., Veretilo Yu. Biometric database based on HOG structures and BCH codes // Proc. ITS. – 2017. – P. 286–287.