LETTER

Altered Fingerprints Detection Based on Deep Feature Fusion*

Chao XU†, Yunfeng YAN††, Lehangyu YANG†††, Sheng LI††††, *Nonmembers, and* Guorui FENG†a), *Member*

SUMMARY The altered fingerprints help criminals escape from police and cause great harm to the society. In this letter, an altered fingerprint detection method is proposed. The method is constructed by two deep convolutional neural networks to train the time-domain and frequency-domain features. A spectral attention module is added to connect two networks. After the extraction network, a feature fusion module is then used to exploit relationship of two network features. We make ablation experiments and add the module proposed in some popular architectures. Results show the proposed method can improve the performance of altered fingerprint detection compared with the recent neural networks.

key words: *altered fingerprint, spectral attention, connected networks, feature fusion*

1. Introduction

Fingerprint identification has been widely used in visas, customs, criminal investigations. In order to avoid AFIS (automatic fingerprint identification system) -based identification, some criminals change the ridge structure of their fingerprints by cutting, transplanting, burning, etc. The resulting fingerprints are called altered fingerprint shown in Fig. 1. Criminals use altered fingerprint to disturb AFIS in order to get away from the investigation of the judiciary department. In 2014, FBI found 412 cases relating to altered fingerprints [1]. Use of altered fingerprints severely influences the judicial efficiency, thus, the way to detect altered fingerprints is needed.

To detect altered fingerprint, Feng et al. [2] proposed a method to detect altered fingerprint based on fingerprint orientation field. Yoon et al. [3] detected altered fingerprint based on directional field discontinuity and minutiae point distribution features. Ellingsgaard et al. [4], [5] proposed a method that detected altered fingerprint using singular point density and minutiae orientation difference. Haraksim et al. [6] tested the algorithm on two different databases, which extracted feature based on image space quality information and fingerprint orientation field. Lazar et al. [7] evaluated three characteristic performances, including coherence, reliability, and uniformity of orientation field.

(a) Original fingerprint (b) Altered fingerprint

Fig. 1 Original fingerprint and altered fingerprint

In 2018, Jain et al. [8] proposed a method based on deep learning to detect altered fingerprint, and proved that deep learning method was better than methods above. In 2020, Giudice et al. [9] used a single architecture to solve multitasks about altered fingerprints. In 2021, Fattahi et al. [10] used the convolutional long short-term memory network to detect the altered fingerprints. Recently, some powerful CNNs (convolutional neural networks) are proposed, e.g. EfficientNet [11] and ViT [12]. They are both excellent deep learning architectures to fill the classification tasks and not applied to solve the problem about altered fingerprints. The method in Reference [9] and [10] didn't improve the network structure for fingerprint features. But in this paper, we propose an altered fingerprint detection based on deep feature fusion of the time-domain and frequency-domain feature. We call it SAC2NETS (spectral attention connecting two networks), and achieve a good performance at the moment. The contributions of the paper are as follows.

- The frequency-domain feature of fingerprints is firstly used to detect the altered fingerprints, which are different from the time-domain feature. We use the real part and imaginary part of the frequency spectrum to represent the frequency-domain information to extract complete feature.
- We design a two-channel network in the field of altered fingerprint detection to train the time-domain and frequency-domain features of fingerprints at the same time, and the real and imaginary part of the frequency spectrum are trained by the same frequency-domain channel network.
- A spectral attention module is proposed to connect the two channels of the network. which combines the time-domain and frequency-domain features in the extraction network to improve the effect of altered fingerprint detection.

Manuscript received March 14, 2022.
Manuscript revised May 29, 2022.
Manuscript publicized June 13, 2022.

†The authors are with School of Communication and Information Engineering, Shanghai University, China.
††The author is with College of Electrical Engineering, Zhejiang University, China.
†††The author is with University of Macau, China.
††††The author is with School of Computer Science, Fudan Univeristy, China.

*This work was supported in part by Science and Technology Planning Project of Zhejiang Province under Grant (2022C01090), the Natural Science Foundation of China under Grant (62072295, 62001416, 62072114), China Postdoctoral Science Foundation under Grant (2020M676719) and Natural Science Foundation of Zhejiang Province under Grant (Q21F030038).

a) E-mail: fgr2082@aliyun.com

DOI: 10.1587/transinf.2022EDL8028

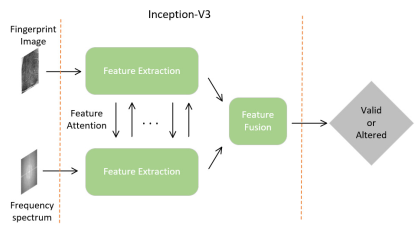


Fig. 2 Altered fingerprint detection flow chart

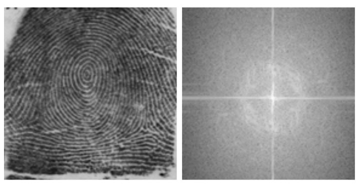


Fig. 3 Fingerprint images and its spectrogram

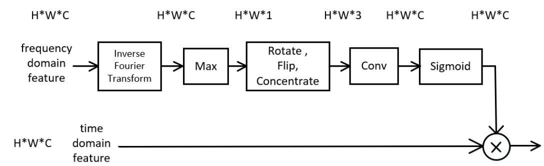


Fig. 4 Complete steps of the spectral attention

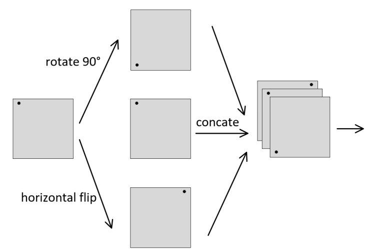


Fig. 5 The step of rotating the frequency-domain feature and concatenate them in the spectral attention module

2. Altered Fingerprint Detection

The framework of the proposed method is shown in Fig. 2. Given a fingerprint image and its spectrogram, feature extraction module is used to extract deep feature from them separately. An attention structure with its spectrogram is added into the fingerprint image extraction network. Then we form a 2048-dimensional fusion feature. Based on fusion feature, the classifier can calculate the score to determine whether it is a real fingerprint or an altered fingerprint.

2.1 Fingerprint Spectrogram

The fingerprint has clear structure, which causes its spectrogram to be very characteristic. As shown in Fig. 3, the detail of the spectrogram concentrates in the middle area on the graph. The frequency spectrum is calculated by Eq. (1):

$$F(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y) \cdot e^{-j2\pi(\frac{ux}{N}+\frac{vy}{M})} \tag{1}$$

where $F(u,v)$ represents the frequency spectrum, $f(x,y)$ represents the fingerprint and j is the imaginary unit.

The spectrogram is calculated by taking the square root of the sum of the real and the imaginary part square.

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)} \tag{2}$$

where $|F(u,v)|$ represents the spectrogram of the fingerprint, $R(u,v)$ represents the real part and $I(u,v)$ represents the imaginary part of $F(u,v)$.

The real part and imaginary part of the frequency spectrum are both important. We directly use two parts to represent the spectrogram to avoid the loss caused by calculating the square root. $R(u,v)$ and $I(u,v)$ are respectively input into the network for training, and the frequency-domain feature is extracted to assist in the detection of altered fingerprints.

2.2 Spectral Attention

Because both time-domain and frequency-domain features have important information. We propose a spectral attention, which is to fuse time-domain and frequency-domain features in the middle of the network. The following introduce steps of the spectral attention shown in Fig. 4. Firstly, the frequency-domain feature is transformed to time-domain by inverse Fourier transform, shown in Eq. (3).

$$\begin{aligned} y &= max(f(x,y)) \\ &= max(\frac{1}{MN}\sum_{u=0}^{N-1}\sum_{v=0}^{M-1} F(u,v) \cdot e^{j2\pi(\frac{ux}{N}+\frac{vy}{M})}) \end{aligned} \tag{3}$$

where y represents the max value of the transformed frequency-domain feature. Secondly, we rotate y 90° and flip y to generate two new features, then concatenate them with y shown in Eq. (4) and Fig. 5.

$$\widetilde{y} = \sigma(\delta(y, y', y'')) \tag{4}$$

where y' represents the feature that rotate 90° of y, y'' represents the feature that flip y, σ represents convolutional and Sigmoid functions and δ represents the operation to concatenate y, y', y''.

At last, we make attention to the original time-domain feature. The original time-domain feature is multiplied by transforming time-domain feature as Eq. (5).

$$\widetilde{x} = x \cdot \widetilde{y} \tag{5}$$

where x represents the original time-domain feature and $\widetilde{x}$ represents the new time-domain feature.

2.3 Two Connected Networks

The main network is divided into two parts, i.e. the time-domain feature and frequency-domain feature extraction

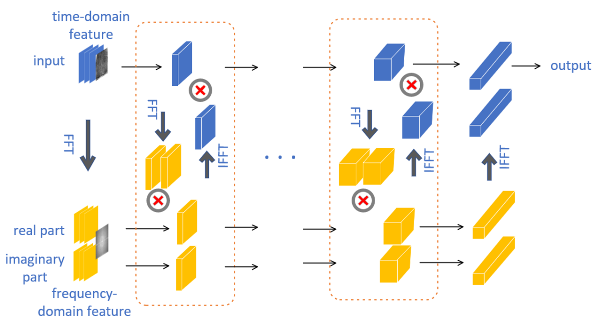


Fig. 6 The main part of the two feature extraction networks

networks. Corresponding the time-domain and frequency-domain features are extracted. The two networks are connected by the attention module which can fuse the above two features. The proposed networks SAC2NETS are shown in Fig. 6.

2.4 Construction of Deep Feature Fusion Network

Feature extraction module is used to extract deep features of fingerprint images and difference maps. It consists of two modified parallel Inception_v3 networks [13], which is proposed by Google. Feature extraction module can extract 2048-dimensional deep features from fingerprint image and frequency spectrum respectively.

In feature fusion module, the deep features of fingerprint image and difference map are fused by the linear weight in Eq. (6). At last, the 2048-dimensional fusion feature is obtained and then imported to the classifier module.

$$F = \alpha_1 F_1 + \alpha_2 F_2 \tag{6}$$

where F_1 and F_2 represent two kinds of feature, α_1 and α_2 represent two learnable weights. The classifier module is used to map fusion features to the sample label space. Moreover, a binary classifier is constructed using cross entropy loss function to classify true fingerprint and altered fingerprint. The loss function is shown in Eq. (7).

$$\mathcal{L} = \frac{1}{N}\sum_i -[y_i \cdot log(p_i) + (1 - y_i) \cdot log(1 - p_i)] \tag{7}$$

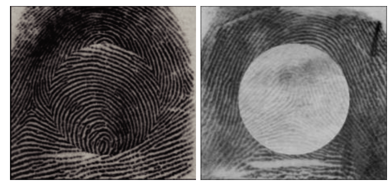
where $\mathcal{L}$ is the average loss, y_i represents the label of sample i, p_i represents the probability that sample i is predicted to be a positive class.

3. Experiment and Analysis

3.1 Database

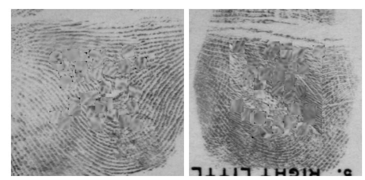
Because there is no open altered fingerprint database, we use the method in [2] to construct the altered fingerprint database. The original fingerprint database is NIST Special Database4 [14] which contains 2000 different fingerprints. The altered fingerprint database contains four kinds of altered fingerprints: Z-CUT, global rotation, central rotation

(a) Z-CUT and Global rotation



(b) Central rotation and transplantation

Fig. 7 Different types of altered fingerprint



(a) Original and Altered fingerprint

Fig. 8 Attacked fingerprint

and central transplantation. Z-CUT is the fingerprint that its center is trimmed into two isosceles triangles, and the two isosceles triangles are spliced into rectangles according to their long sides. Central rotation is the whole fingerprint that rotated for 180 degrees. Global rotation is the fingerprint that its central part is rotated for 180 degrees. Central transplantation is the fingerprint which its central part is transplanted by another fingerprint.

The four types of altered fingerprints are shown in Fig. 7. We divide the original fingerprints into four groups, and each group is performed an altered pattern. The original fingerprints and altered fingerprints are flipped horizontally and vertically to four times. In order to increase the practicability of identification, we add some random attacks to the datasets, such as slight distortion and blur. Attacked original fingerprint and altered fingerprint are shown in Fig. 8.

3.2 Experimental Settings

We use PyTorch deep learning framework for experiments. The hardware environment is a computer equipped with a NVIDIA GeForce GTX 2070 8 GB graphics card, 16 GB RAM and an Intel Core i7-8700k CPU. The database is randomly divided into the training set (40%), validation set (20%), and testing set (40%). The methods used in the paper are all trained by the same database we construct and adopted the same percentage of the data.

3.3 Experimental Result and Analysis

To prove the effectiveness of deep feature fusion, we com-

Table 1 The accuracy comparison (%) between the method in [9] and SAC2NETS

Method	Method in [9]	SAC2NET
Accuracy(%)	97.43	**97.96**

Table 2 The accuracy comparison (%) among the rotation angel in the attention module

Rotation angel	90°	180°	270°	Flip	90°+Flip	All
Accuracy (%)	97.72	97.66	97.71	97.66	**97.96**	97.92

Table 3 The accuracy comparison (%) among different stage of the resnet-50 [15] with SAC2NETS

Method	Accuracy (%)
Resnet-50	95.36
stage 1 + SAC2NETS	96.23
stage 2 + SAC2NETS	96.21
stage 3 + SAC2NETS	96.09
All + SAC2NETS	**96.86**

pare the detection performance of the method proposed with that in [9] and the result is shown in Table 1. The performance of method proposed is 0.53% higher than one in [9]. The frequency-domain feature is also effective in the altered fingerprint detection. After training, it can distinguish the high and low frequencies. Therefore, the spectral attention module to fuse the time-domain and frequency-domain features can extract the feature better.

We make ablation experiments to gain a better understanding of the proposed method. We first study the influence of rotation angel of the frequency-domain feature in the spectral attention module. We compare the influence among rotating the feature map 90°, 180°, 270° and flipping it. Table 2 shows the method combining the features rotated 90° and flipped together has the best performance. It is nearly 0.15% higher than rotating or flipping the feature, because the frequency-domain features in different directions have more information than in one direction. Since the feature has the central symmetry, it is the same as rotating it 180°.

We next explore the influence of SAC2NETS at different stages by integrating it into ResNet-50 [15]. We add SAC2NETS to the different stages of the architecture, and report the results in Table 3. It can be seen that the accuracy is higher when SAC2NETS is added to the front stage of the network, and it obtains the best performance when SAC2NETS is added to all stages. We consider frequency-domain features in the front stage of networks have more complete spectrum information.

Finally, we study the effect of adding SAC2NETS to some other popular architectures, e.g. Res2Net-50 [16], EfficientNet [11] and Vit [12]. We can observe the results in Table 4 that the other architectures with SAC2NETS also have improvement. Res2Net-50 with SAC2NETS has an accuracy of 0.58% gain which is superior to Res2Net-50. EfficientNet with SA2NETS has an accuracy of 0.14% gain which is superior to EfficientNet. Vit with SAC2NETS proposed has an accuracy of 0.22% gain which is superior to its direct counterpart. Vit is a new method with transformer, which is different from CNN. Since the size of feature in Vit is not fit to make FFT, we only add the spectral attention once in the first half of the network and the improvement is not obvious. EfficientNet with SAC2NETS has the best result which achieves 98.49% detection accuracy.

Table 4 The accuracy comparison (%) among some other popular aritectures, Res2Net [16], EfficientNet [11] and Vit [12] which are added the method proposed

Method	Original	Method + SAC2NETS
Res2Net	97.47	98.05
EfficientNet-b2	98.35	**98.49**
Vit	96.67	96.89

4. Conclusion

In this paper, an altered fingerprint detection method called SAC2NETS is proposed. The method trains two deep feature fusion networks. Feature extraction module is constructed by two modified backbone networks and used to extract deep feature of fingerprint images and frequency spectrum. A spectral attention is added in extraction module, which connects two networks and exchanges information to help extract features. After extraction module, two kinds of features are integrated with learnable weights to calculate the category. Results show the backbone networks with SAC2NETS all have improvement in altered fingerprint detection.

References

[1] A. Fingerprints, "A challenge to law enforcement identification efforts," FBI Law Enforcement Bulletin, 2015.
[2] J. Feng, A.K. Jain, and A. Ross, "Detecting altered fingerprints," 2010 20th Int. Conf. Pattern Recognit., pp.1622–1625, IEEE, 2010.
[3] S. Yoon, J. Feng, and A.K. Jain, "Altered fingerprints: analysis and detection," IEEE Trans. Pattern Analysis & Machine Intelligence, vol.34, no.3, pp.451–464, March 2012.
[4] J. Ellingsgaard, C. Sousedik, and C. Busch, "Detecting fingerprint alterations by orientation field and minutiae orientation analysis," 2nd International Workshop on Biometrics and Forensics, pp.1–6, IEEE, 2014.
[5] J. Ellingsgaard and C. Busch, "Altered fingerprint detection," in Handbook of Biometrics for Forensic Science, pp.85–123, Springer, 2017.
[6] R. Haraksim, A. Anthonioz, C. Champod, M. Olsen, J. Ellingsgaard, and B. Christophe, "Altered fingerprint detection–algorithm performance evaluation," 2016 4th Int. Conf. Biometrics and Forensics (IWBF), pp.1–6, IEEE, 2016.
[7] C. Lazar, C.D. Psenita, and A. Tiganasu, "Comparative analysis of orientation field descriptors used for detecting altered fingerprints," 2016 20th Int. Conf. System Theory, Control and Computing (ICSTCC), pp.715–720, IEEE, 2016.
[8] E. Tabassi, T. Chugh, D. Deb, and A.K. Jain, "Altered fingerprints: Detection and localization," 2018 IEEE 9th Int. Conf. Biometrics Theory, Applications and Systems (BTAS), pp.1–9, IEEE, 2018.
[9] O. Giudice, M. Litrico, and S. Battiato, "Single architecture and

multiple task deep neural network for altered fingerprint analysis," 2020 IEEE Int. Conf. Image Process. (ICIP), pp.813–817, IEEE, 2020.

[10] J. Fattahi and M. Mejri, "Damaged fingerprint recognition by convolutional long short-term memory networks for forensic purposes," 2021 IEEE 5th Int. Conf. Cryptography, Security and Privacy (CSP), pp.193–199, IEEE, 2021.

[11] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," Int. Conf. Mach. Learn., pp.6105–6114, PMLR, 2019.

[12] A. Dosovitskiy, L. Beyer, A. Kolesnikov, D. Weissenborn, X. Zhai, T. Unterthiner, M. Dehghani, M. Minderer, G. Heigold, S. Gelly, J. Uszkoreit, and N. Houlsby, "An image is worth 16x16 words: Transformers for image recognition at scale," arXiv preprint arXiv:2010.11929, 2020.

[13] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," Proc. IEEE Conf. Comput. Vis. Pattern Recognit., pp.2818–2826, 2016.

[14] C.I. Watson and C. Wilson, "Nist special database 4," Fingerprint Database, National Institute of Standards and Technology, vol.17, no.77, March 1992.

[15] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," Proc. IEEE Conf. Comput. Vis. Pattern Recognit., pp.770–778, 2016.

[16] S.H. Gao, M.M. Cheng, K. Zhao, X.Y. Zhang, M.H. Yang, and P. Torr, "Res2net: A new multi-scale backbone architecture," IEEE Trans. Pattern Anal. Mach. Intell., vol.43, no.2, pp.652–662, Feb. 2021.