International Journal on Semantic Web and Information Systems
Volume 19 • Issue 1

PRNU Anonymous Algorithm Used for Privacy Protection in Biometric Authentication Systems

Jian Li, Qilu University of Technology (Shandong Academy of Sciences), China*

Xiaobo Zhang, Qilu University of Technology (Shandong Academy of Sciences), China

Bin Ma, Qilu University of Technology (Shandong Academy of Sciences), China

Meihong Yang, Shandong Computer Science Center, China

Chunpeng Wang, Qilu University of Technology (Shandong Academy of Sciences), China

Yang Liu, Qilu University of Technology (Shandong Academy of Sciences), China

Xinan Cui, ZhongFu Information Inc., China

Xiaotong Yang, Sungkyunkwan University, China

ABSTRACT

The photo response non-uniformity (PRNU) is used to connect an image to its source sensor. In this paper, researchers propose a PRNU anonymity method based on image segmentation to cut the relationship between the image and its source camera. According to the distribution rule of PRNU in the high and low frequency band of the image, the high and low frequency information of the part is also processed differently, which ensures the quality of the output image to a large extent. Experiments on the datasets show that the proposed method can preserve the biometric characteristics of the device while maintaining the anonymity of the device. Comparing with prior art, peak signal to noise ratio (PSNR) and cosine similarity are improved by 1.9 dB and 0.02 points, respectively.

KEYWORDS

Biometric Recognition, Digital Image Forensics, Discrete Wavelet Transform, Maximum Likelihood Based PRNU Estimation, PRNU Noise, Sensor De-Identification, Source Identification, Wiener Filtering

INTRODUCTION

Privacy might leak when people hand their personal images or videos to an authentication system for entrance permission (Narang et al., 2020). Traditional solutions usually focus on the protection of multimedia contents—for instance, faces. However, the device that is used to capture an image can expose one’s privacy, too. Sensor pattern noise (SPN)-based algorithms are able to distinguish a camera and then find the owner, raising a host of new questions about personal privacy and anonymity. Therefore, it is particularly important to anonymize the source attributes of an image while preserving the biometric utility in some specific biometric scenarios.

DOI: 10.4018/IJSWIS.317928

*Corresponding Author

Limitations of Prior Art

Device anonymization needs us to remove the SPN from image. The main component of SPN is photo response non-uniformity (PRNU) noise. PRNU is a signal with a rather wide frequency spectrum. In this light, an appropriate frequency domain analysis method is important to achieve the balance between the PRNU anonymization and high image quality.

The traditional PRNU masking method has the following disadvantages:

- In the classical Fourier Transform domain, the signal expression is not intuitive, and the suppression effect of PRNU is weak. The compression based on discrete cosine transform (DCT) generally appears as a block effect, which will affect the image quality.
- For biometric images, the existing anonymous algorithms are more complex and require a large number of expensive training images. Therefore, anonymous methods need to be balanced and efficient in practical applications.

Proposed Work

Generally, the area around the edge is misunderstood when only weaker noise filters are used, such as Wiener filters or median filters. The residual noise obtained by the wavelet transform filter also contains the fewest scene features. Therefore, an edge filter based on wavelet and Wiener filters is selected.

In this paper, we propose a simple method to anonymize the device while preserving biometric utility. The approach we propose has two dimensions. First, the original image is separated from the eyes or face. In view of the different levels of importance of the human eye (or face) and other regions in a biometric image for identity recognition, we conduct eye separation to strengthen the identity pass rate. Second, the image anonymity is carried out.

Advantages Over the Prior Art

The object of our work is to develop an algorithm to cover the sensor fingerprint (PRNU) while preserving the visual quality and biometric utility. The advantages of the proposed method are as follows:

1. An algorithm based on discrete wavelet transform (DWT) is proposed, which can perform different processing for high- and low-frequency bands of PRNU hierarchically. This algorithm ensures that anonymity has a higher success rate even in light conditions.
2. Image segmentation is applied to ensure that the processed test image preserves more original details. In particular, its biometric content achieves only slight degradation, preserving more biometric utility of the image.
3. This method not only achieves the anonymity of PRNU but also overcomes some defects of existing algorithms. The PSNR and cosine similarity between the output image and the original image are improved by 2.4 dB and 0.1 percentage points on average, respectively.

The rest of this paper is organized as follows. We introduce some methods about the traditional PRNU anonymity and PRNU extraction. We then describe the proposed method for PRNU anonymization. Next, we describe the datasets, experimental results, and comparisons. We then show the future development and application of this work and conclude the paper.

BACKGROUND

PRNU Extraction

The special marks left in an image by the camera's sensor, named PRNU noise, is a device fingerprint used to attribute an image or video to its capturing device (Mandelli et al., 2020). Lukas et al. (2006)

proposed the first popular PRNU extraction algorithm. However, this algorithm did not consider that PRNU was related to image content. Chen et al. (2008) extended Lukas et al.'s method by using a method based on a reasonable camera sensor output model to divide an image I into three parts as shown in equation (1):

$$I = I^{(0)} + I^{(0)} \cdot K + \theta \tag{1}$$

In equation (1) $I^{(0)}$ is an ideal image without any noise, K is a multiplicative factor that contains PRNU noise, and θ represents all the rest noises, such as distortion owing to image compression and modeling error. Then a maximum likelihood estimation method was proposed for the extraction of camera PRNU's multiplicative factor K. This method is shown in equation (2):

$$\widehat{K} = \frac{\sum_{k=1}^{m} w^k I^k}{\sum_{k=1}^{m} (I^k)^2} \tag{2}$$

On the basis of maximum likelihood estimation, there are many methods to extract PRNU from video. Ma et al. (2021) proposed a new patch-based matching strategy that was unlike most previous methods that tended to match PRNU within the entire frame.

Prior Arts for PRNU Anonymization

PRNU anonymization can be implemented in two different ways. The first method relies on weakening the PRNU fingerprint by strong filtering or compression (López et al., 2020). Bhme and Kirchner (2013) proposed a method based on flat-fielding to suppress PRNU noise. However, this approach was not applicable to most consumer cameras that do not support raw format output. Hence, Ahmet et al. (2014) proposed an adaptive PRNU denoising method that can remove a PRNU fingerprint without compromising image quality significantly in terms of PSNR. Karaküçük and Dirik (2015) improved on existing adaptive PRNU denoising methods and provided a benchmark against other PRNU anonymization. Hui et al. (2016) proposed an attack method by estimating the intrinsic strength of PRNU and removing its fingerprint from the target image. Recently, deep learning has become popular for PRNU suppression. Bonettini et al. (2018) focused on the possibility of editing images in visually imperceptible ways to prevent PRNU noise estimation through convolutional neural networks (CNN). Picetti et al. (2022) designed a deep learning-based approach to suppress PRNU traces. They transformed PRNU anonymization into a combination of global optimization and local post-processing problems in the Depth Image First (DIP) framework.

The second anonymous method focuses on the interference alignment between the test PRNU and reference PRNU, including resize, rotation, cropping, and other operations. Bayram et al. (2013) proposed an algorithm based on seam carving to change the pixel position, but this method ignored the influence of the high-gradient image region on the PRNU registration. To address this problem, Dirik et al. (2014) proposed a forced seam removal method so that the process does not leave many blocks uncarved. Recently, Taspinar et al. (2020) proposed a general hybrid media matching algorithm to solve the problem of PRNU-based source camera properties becoming invalid when media are of different types or PRNU cannot be aligned.

Because of the enhanced robustness of current de-identification algorithms (Li et al., 2019), the anonymity of biometric (face, iris, fingerprint) images is required to be higher. Newton et al. (2005) proposed a new privacy-enabling algorithm, called k-Same, that guarantees faces cannot be reliably recognized. In addition, methods based on deep learning are also popular in this field. Zhang et al. (2020) classified the typical face anti-spoofing algorithms twice and analyzed their basic ideas and advantages and disadvantages. Ju (2020) reviewed the deep learning detection models for face manipulation in recent years. In addition, Liu and Chen (2020) discussed the face detection methods generated by generative adversarial networks (GANs) and analyzed the advantages and disadvantages of these models according to the network structure and evaluation indicators, as well as the results obtained on their respective datasets.

The above works are mainly to prevent the privacy disclosure of a facial image and its attribute data, but few studies had been carried out on the protection of source devices. So Banerjee et al. (2019) proposed an iterative perturbation algorithm that applied patch-based modifications to the input biometric image to perform sensor spoofing while retaining its biometric utility. Furthermore, Banerjee and Ross (2020) recently developed a fairly simple, noniterative algorithm method by applying DCT to images and further changed DCT coefficients to achieved PRNU deception and anonymity while preserving biometric utility. However, the robustness of this algorithm was shown to be weak in the Visio database (Li et al., 2020).

PROPOSED METHOD

As shown in Figure 1, the proposed method in this article consists of two modules. The first module is eye or face segmentation. It is mainly to segment the eye or face region from the original image, which is prepared for the anonymous algorithm. Here we use human eye segmentation as an example to illustrate. The second module is the main partition of PRNU inhibition: PRNU anonymization.

Eye Segmentation

For part of the eye image or face image, the area generally includes two parts. One is the eye or the face area and the other background area. The two regions play different roles in identity. Based on this, we suggest that the face or eye area of high importance should be stripped and segmented first. Then it makes fewer modifications to its pixels to ensure the final recognition pass rate.

We use the cascade object detector in the MATLAB toolbox for object detection to obtain *Eye image*. Its core is the Viola-Jones algorithm. The dashed line of module 1 in Figure 1 shows the specific flow of this algorithm. The Viola-Jones object detection algorithm uses Haar eigenvalues for object detection and generates a cascade classifier through the Adaboost algorithm to directly match features in a small area of the image to determine whether there is a human eye in the area.

First, an integral graph is a computational method to speed up the box filtering or convolution process. The value of any point in the integral image is equal to the sum of all pixels in the upper left corner of that point. Figure 2 is an example of an integral graph computation.

In Figure 2 the sum of the pixels within rectangle D can be computed with four array references. The value of the integral image at location 1 is the sum of the pixels in rectangle A. The value at location 2 is A+B, and at location 3, it is A+C. At location 4 the value is A+B+C+D. The sum within D can be computed as 4+1-(2+3).

After integral graph operation about an image is completed, the integral graph computation calculates Haar eigenvalues. Different eigenvalues mean different things. We can carry out feature extraction according to the uneven distribution of Haar eigenvalues in the sample.

The cascade classifier constructed by the Adaboost method is used to detect eyes in the image window. We need to scale the image according to a certain size scale factor. The cascade classifier then hands the detection window to the first-level classifier. If the detection window does not contain human eyes, the classifier will discard the detection window and stop the detection. If the current detection window is judged to contain eyes, the lower-level classifier will continue the detection.

Finally, the non-maximum suppression (NMS) algorithm is carried out. The candidate boxes are merged and filtered to find the best eye detection position. Figure 3 shows the automatic segmentation results of some images in the MICHE-I dataset.

Figure 1. The flowchart of the proposed method (The First Module Is Eye Segmentation, and the Second Module Is PRNU Anonymization)

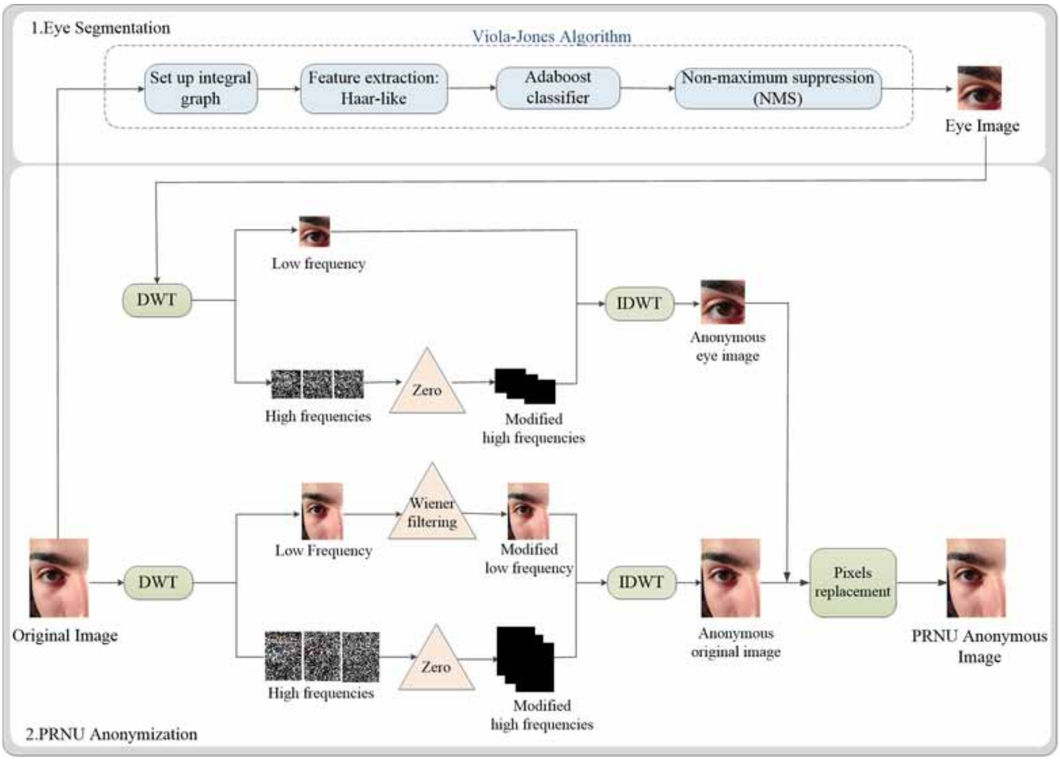
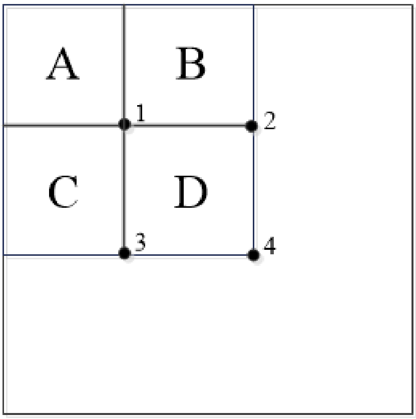


Figure 2. An integral graph computation

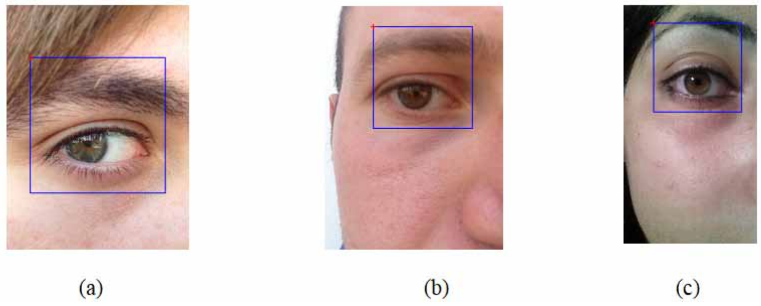


PRNU Anonymization

This module is mainly divided into two parts. The first part is PRNU anonymity in the Eye image. The second section is PRNU anonymity in the original image.

The module is implemented in the DWT domain of the image. An example of decomposing an image with three layers of DWT is shown in Figure 4. It is well known that PRNU is mainly related

Figure 3. An example image of an eye segmentation result

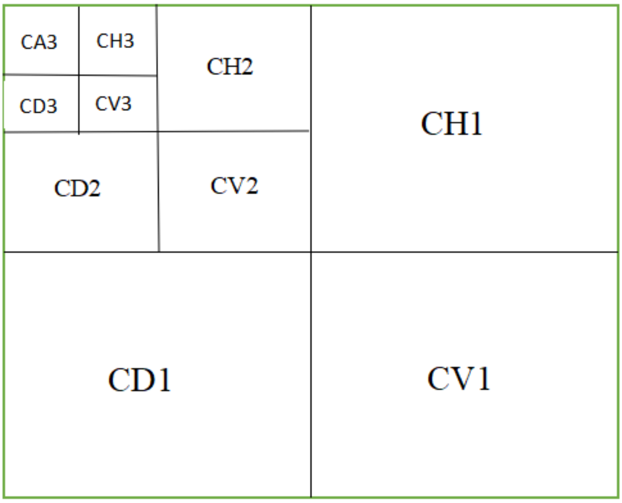


to the medium- and high-frequency components of the image. Therefore, we recommend strong suppression for high frequencies and weak suppression for low frequency.

Figure 4 shows the decomposition of a three-layer wavelet transform. CA_3, CH_i, $CV_{i,}$ and CD_i *(i=1,2,3)*, respectively, represent the low-frequency component, horizontal intermediate frequency (IF) component, vertical IF component, and diagonal high-frequency component of an image:

- **Eye image:** The given eye image is E. The image is generally the output image of module 1, and the position information $(x:x_1, y:y_1)$ is generated in the original image during the process. We first subject t image to DWT to yield E_{dwt}. To ensure that the features around the eyes of the object in the image are not damaged, we do not process the decomposed low-frequency E_{low}. The high-frequencies E_{high} are set to zero. The anonymous eye image E_0 is then obtained by applying the inverse DWT. Algorithm 1 describes these steps.
- **Original image:** The given for the original image is I. Compared with an image of the eye region, the importance level of the other region for identity recognition is weak. Therefore, we perform (k+1)-layer DWT to yield I_{dwt}. We aim to achieve efficient anonymity without compromising low-frequency details. To achieve this goal, we added a Wiener filtering with a

Figure 4. Decomposing an image with three layers of DWT



3×3 window to the low-frequency I_{low}. The results show that slight filtering is effective in suppressing PRNU in the low-frequency band. As shown in Figure 5, the visual quality of an image before and after filtering will not be greatly affected. Unlike I_{low}, the high frequencies I_{high} are set to zero. The inverse DWT is applied to obtain an anonymous original image. Next, its pixel values in the eye region will be changed to the pixel values of E_0—namely, $I(x : x_1, y : y_1) = E_0$. Finally, the PRNU anonymous image I_0 will be obtained. Algorithm 1 describes these steps.

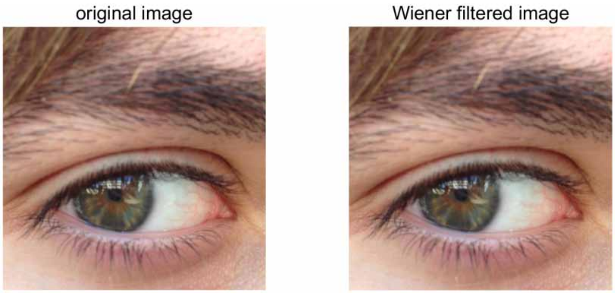
EXPERIMENTS AND RESULTS

The experiment of this work is mainly carried out in the following two aspects. The first is to test the performance of algorithm 1 on PRNU anonymity. The second is carrying out the biometric matching experiment. We considered the periocular matcher in this experiment because many of the images used in this work are partial facial images. The gallery images are the original images, and the probe images are the modified images. The score (positive score or negative score) of two sample images (belonging to the same object or not) is calculated, and the category of confusion matrix is judged by different thresholds.

Datasets

We use the Mobile Iris Challenge Evaluation (MICHE-I) dataset (Marsico et al., 2018) and face dataset for performing experiments. The MICHE-I dataset comprises more than 3,000 eye images from different devices (Galdi et al., 2016). We employ the periocular images from two smartphones in this dataset: Apple iPhone 5 and Samsung Galaxy S4. Galdi et al. (2016) showed that two separate units of Apple iPhone 5 were used for data collection. We refer to them as “UNITI” and “UNITII,” respectively. Furthermore, we acquired the images in this dataset using the front and rear camera sensors separately. Thus, the MICHE-I dataset used in this work consists of data from six sensors. Some examples of periocular images are shown in Figure 6. We represent Apple iPhone 5 device as “Device1” and Samsung Galaxy S4 device as “Device2.” The face dataset is created by the Shandong Provincial Key Laboratory of Computer Networks. These included about 500 facial images taken using the front and rear cameras of three different devices: the Apple 14Pro, Huawei Honor, and Redmi K30. These images include different lighting and background scenes. Table 1 describes the specifications of the two datasets.

Figure 5. An Image Comparison Before and After Wiener Filtering. (a) Original image; (b) Wiener-filtered image.



Algorithm 1. Anonymous methods

```
Eye segmentation
Input: An image $I$
Output: An eye image $E$ of $I$
1. Build an integral image of I to get an array of rectangular features.
2. Calculate the Haar eigenvalue according to the array.
3. Apply Gadabouts classifier to detect and judge eyes.
4. Apply NMS optimize windows to obtain $E$ and position information $\left(x : x_1, y : y_1\right)$.
5. Return the extracted eye image $E$.
PRNU Anonymization
Input: The image $I$, $E$, and $\left(x : x_1, y : y_1\right)$
Output: PRNU anonymous image $I_0$
1. Apply k-dimensional DWT to $E$ to obtain high and low frequency ($H_{eight}$ and $E_{low}$)
       $E_{high}$, $E_{low}$ = DWT ($E$)
2. for wavelet decomposition levels do
        for wavelet components in $E_{high}$ do
            $E_{high}$ (:)==0
3. Apply inverse DWT to obtain the modified image $E_0 = \mathrm{DWT}^{-1}(E_{low}', E_{high})$
4. Return the modified eye image $E_0$
5. Apply (k+1)-dimensional DWT to $I$ to obtain high and low frequency ($I_{high}$ and $I_{low}$)
       $I_{high}$, $I_{low}$= DWT ($I$)
6. Apply the Wiener filter to $E_{low}$ in highest level.
       $E_{low}$'=WF($E_{low}$)
7. for wavelet decomposition levels do
        for wavelet components in $I_{high}$ do
            $I_{high}$ (:)==0
8. Apply inverse DWT to obtain the modified image $I_0 = \mathrm{DWT}^{-1}(I_{low}, I_{high})$
9. Return the modified image $I_0$
```

We split the dataset into a training set and a test set and followed the topic separation protocol to create a training set and a test set. The training set of this work consists of 30% of the total number of images taken by each camera sensor from the MICHEI dataset. The training set is used to generate a reference pattern for each sensor, as shown in column 5 of Table 1. The test set accounts for 70% of the total number of images taken by each camera, and these images are used to experiment with anonymous algorithms.

Figure 6. Example images from the MICHE-I dataset acquired using (A) Apple Iphone 5 UNITI front, (B) Apple Iphone 5 UNITI rear, (C) Samsung Galaxy S4 front sensors

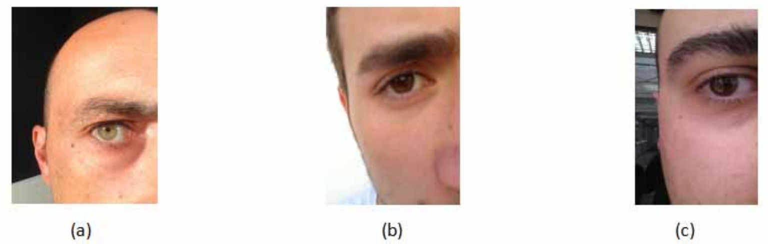


Table 1. Dataset specifications

Smartphone	Device Identifier	Sensor	Image Size	Training Set/ Total Number of Images	Test Set/Total Number of Images
Apple iPhone 5	Device1	Front(F)	960×1280	119/397	278/397
	UNITI	Rear(R)	1536×2048	125/411	289/411
Apple iPhone 5	Device1	Front(F)	960×1280	67/222	155/222
	UNITII	Rear(R)	2448×3264	67/229	162/229
Samsung Galaxy S4	Device2	Front(F)	1080×1920	195/637	442/637
	UNITI	Rear(R)	2322×4128	198/660	462/660
Apple iPhone14 Pro	Device3	Front(F)	3024×4032	28/88	60/88
		Rear(R)	3024×4032	29/89	60/89
LGE-AN00	Device4	Front(F)	4096×3072	24/81	57/81
		Rear(R)	4096×3072	24/80	56/80
Redmi K30	Device5	Front(F)	3880×5184	24/82	58/82
		Rear(R)	3472×4624	24/75	51/75
Total				924/3051	2130/3051

Performance Criteria

We use four criteria to evaluate the experimental results. First, the peak correlation energy (PCE) is used to determine the relationship between the output anonymous image and its reference PRNU. This formula is shown in equation (3):

$$PCE(R,W) = \frac{C_{RW}^{2}(0,0)}{\frac{1}{MN-\left|A\right|}\sum_{(K,L)\notin A} C_{RW}^{2}(k,l)} \tag{3}$$

In equation (3) C_{RW} is the $2D$ cyclic cross-correlation between an anonymous image R and its PRNU W, A is the small region around (0,0), and $|A|$ is the cardinal number of the region. An appropriate threshold value is selected to judge the effectiveness of the algorithm. If the PCE is greater than the threshold, the anonymized image is considered to have no connection to its PRNU. Otherwise, it is considered to have a connection. In the proposed method, we set the PCE threshold to 20.

Second, we used the PSNR metric to judge the quality of the image. Generally, the human eye cannot distinguish whether the image is disturbed when the PSNR is above 36 dB. With PSNR below 36 dB, we can clearly see the difference between the interference and the original image. Here we think that the higher the PSNR metric, the closer it is to the purpose of this experiment. It first calculates the mean square error (MSE) with the anonymized image and then uses it to define the PSNR, as shown in equations (4) and (5):

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} || \, I(i,j) - K(i,j) \, ||^2 \tag{4}$$

$$PSNR = 20 * \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \tag{5}$$

In equations (4) and (5) I is the original image, K is the image after interference, and MAX_I represents the maximum value of the pixel. For example, if each sampling point is represented by 8 bits, then it is 255.

Third, we used the cosine similarity to test whether the anonymous image changes its ability about face recognition. Cosine similarity refers to the cosine of the angle between two objects and is used to measure the difference. The closer this value is to 1, the better we think it will be. We employed the ResNet101 (He et al., 2016) architecture pretrained on ImageNet (Kornblith et al., 2018) dataset for performing periocular matching. The features of the 170th layer are considered the best match (Hernandez-Diaz et al., 2018). The anonymous image is then processed by adaptive histogram equalization, and it is input into CNN. Finally, the cosine similarity between face feature F(B) extracted from the anonymous image and feature F(I) extracted from the original image is calculated as shown in equation (6):

$$similarity = \frac{F(I) \cdot F(B)}{\left\|F(I)\right\|\left\|F(I)\right\|} = \frac{\sum_{i=1}^{n} F(I)_i \times F(I)_i}{\sqrt{\sum_{i=1}^{n}\left(F(I)_i\right)^2} \times \sqrt{\sum_{i=1}^{n}\left(F(I)_i\right)^2}} \tag{6}$$

Finally, recall and precision are applied to evaluate the proposed model. Recall represents how many positive examples in the sample are predicted to be correct. The precision represents how many of the samples predicted to be positive are actually positive. The larger the area under the "precision-recall" curve, the higher the recognition accuracy. We applied the cosine similarity between two objects for classification.

Suppose that in a dataset detection, four types of detection results are generated: TP,TN, FP and FN. In these results, T and F, respectively, represent the results of correct and wrong samples; P and N, respectively, represent the results of predicted samples as positive and negative examples. The confusion matrix composed of the four scenarios is shown in Table 2. So recall and precision can be represented as shown in equations (7) and (8):

Table 2. Confusion matrix

Real Label	Predicted Result	
	Positive example	**Negative example**
True example	TP	FN
False example	FP	TN

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

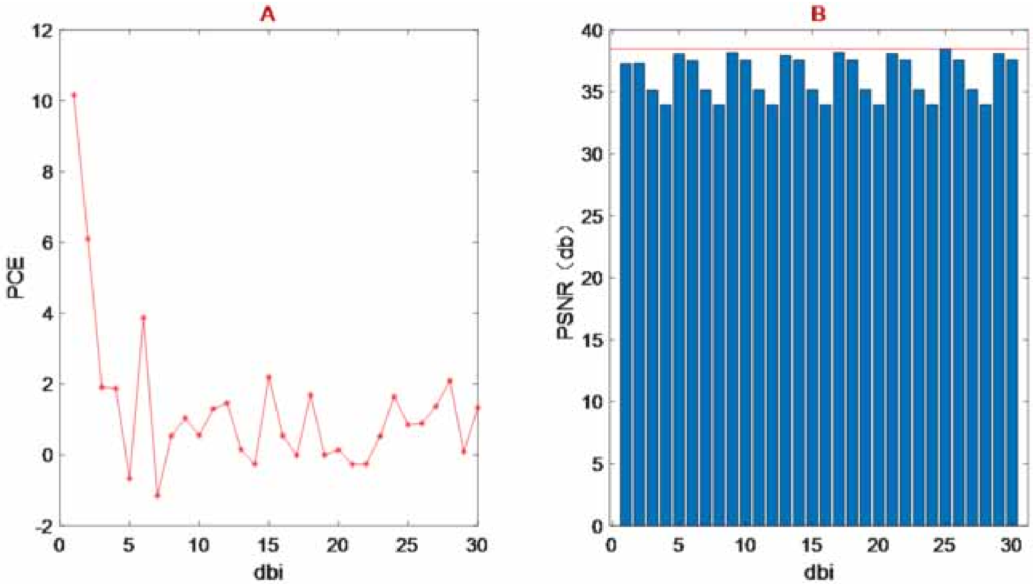
$$Precision = \frac{TP}{TP + FP} \tag{8}$$

The Selection of Wavelet Transform

In this part, we conduct experiments on the wavelet basis function and the number of layers *k* decomposed by DWT, respectively.

First, it is very important to select the wavelet basis function of DWT. Some images of the six sensors in Table 1 are randomly selected. These images account for 20% of the total number of images of the corresponding shooting device. The test experiment of algorithm 1 is then carried out on these random images. The combined effect of the PSNR and PCE means was estimated. Figure 7 shows that the application of the “dbn” wavelet basis function can make the output image’s anonymity successful. Based on this, we chose the wavelet basis function with vanishing distance of 25 to obtain the highest image quality PSNR.

Figure 7. Average results of experiments on random images based on different wavelet basis functions (A represents the average PCE value and B represents the average PSNR value)



Through experiments, we find that a layer of wavelet transform cannot anonymize source devices successfully. In addition, the more layers of wavelet decomposition, the more obvious the inhibition effect of PRNU. Therefore, we compare the experimental effect of three layers of image decomposition based on two layers of wavelet transform. The specific comparison results are shown in Table 3. From the comprehensive index of the three devices, the decomposed two-layer image can achieve better image quality and higher feature retention. Therefore, we set the value of k to 2 in section "PRNU Anonymization".

Comparison of Experimental Results

The purpose of the comparison experiment is to prove that the proposed method can maintain better image quality and similarity under the premise of anonymity. To date, the work on PRNU anonymization about biometric images is very limited, so the presented work is compared with only the state-of-the-art method (Banerjee and Ross, 2020).

There is no doubt that the image will be assigned to the right sensor with high precision. The most important thing is the allocation after interference. When the sensor classifier accepts the modified image as input, the anonymous effect of the two datasets is shown in Figure 8. On the whole, PCE values are concentrated below 20, indicating that the proposed method achieves the effect of anonymity. In the MICHEI dataset, the anonymity rate of sensors all reach 100% except for the "Device1_UNITII_R." The anonymity rate of the Face dataset is 100% except for the "Device5_F." In any case, as shown in Figure 9, the method used by Banerjee and Ross (2020) successfully achieves anonymity in the MICHEI dataset. However, the anonymous effect in the Face dataset is not ideal. It shows that this method has poor scalability.

Table 3. Comparison results after wavelet decomposition

	Samsung Galaxy S4		Apple iPhone 5 UNITI		Apple iPhone 5 UNITII	
	Two-Layer Wavelet Transform	Three-Layer Wavelet Transform	Two-Layer Wavelet Transform	Three-Layer Wavelet Transform	Two-Layer Wavelet Transform	Three-Layer Wavelet Transform
PSNR	39.0504	35.4231	35.4505	33.2646	41.0799	40.9744
Cosine similarity	0.9766	0.9421	0.9713	0.9465	0.9930	0.9910

Figure 8. The PCE of the proposed method (a) the MICHEI dataset (b) the Face dataset

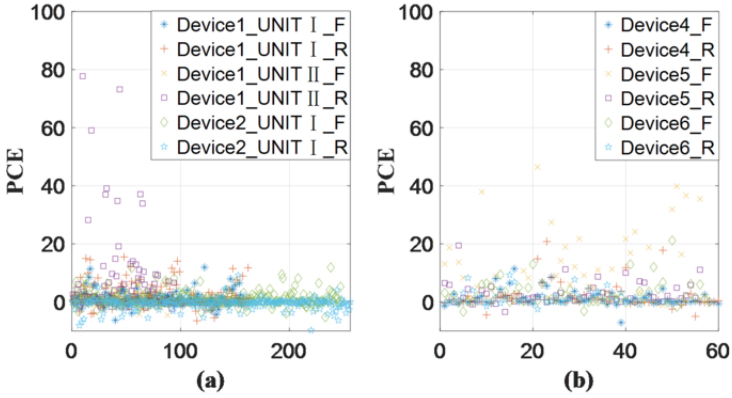


Figure 9. The PCE of the proposed method in the literature (Banerjee and Ross, 2020) (A) the MICHEI dataset (B) the Face dataset

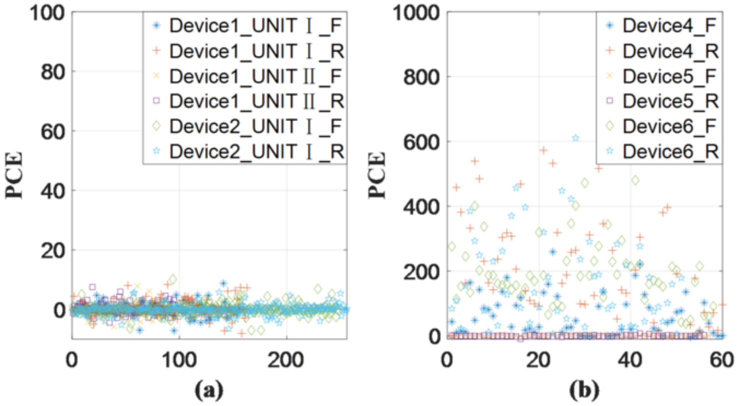


Figure 8 also reflects the situation that the PCE values obtained between different test images of the same device or the same image of different devices are quite different. One of the differences between different devices, such as the "Device1_UNITII_R" and the other devices, is due to the difference in the chip within the device. Different chips more or less affect the persistence of PRNU so that the difficulty of inhibition is also different. We further compared the correlation between the original image and the reference PRNU in this device, and several images of the maximum PCE were undoubtedly from this device. The second reason may be the inconsistent size of images taken between different devices. Among the six devices, the "Device1_UNITII_R" and "Device5_F" have larger size on images. Accordingly, the PCE values are also large. The third is related to the front or rear camera, such as the two devices of the Apple 5. The front camera will have lower pixels than the rear camera, and the front camera will have a blurring function, which will affect PRNU suppression.

In addition, the PCE of different images between the same device may have a certain gap. One reason is related to physical conditions. The datasets include images taken indoors and outdoors, which will have different lighting. Another reason is related to the variance of the image, and a different character has different characteristics—for example, with and without beard. The high frequency of the beard is less suppressed, which will make the correlation larger.

As shown in Figure 10, we further compared the PSNR of the anonymous image and the original image. Figure 10 is a block diagram showing the PSNR values for both approaches. For the MICHEI

Figure 10. The comparison results of PSNR values between our proposed method and the most advanced method proposed by Banerjee and Ross (2020). The upper end of each of the 12 boxes is the maximum value of PSNR, the bottom is the minimum value, and the middle is the PSNR median. (A) the MICHEI dataset (B) the Face dataset.

dataset, the proposed method has obvious advantages. Although some PSNR values are improving, the image quality is still poor (average PSNR<34). We think that the main information in these images occupied a large area. Therefore, most details are removed after further filtering by the anonymous method, resulting in a small PSNR. In addition, the average PSNR value in other sensors can be maintained around 35 dB. This suggests that the image after the attack is not much different from the original image under the naked eye. Figure 11 shows a comparison of an image before and after anonymity. For the Face dataset, the PSNR of the proposed method is lower than the results achieved by Banerjee and Ross (2020) because its anonymity is not successful. With less PRNU removed, image pixels will not change much accordingly.

Because of the limit of anonymous success, we discuss changes in the PSNR only on the MICHEI dataset. The anonymous images obtained by the method based on DCT is about 32 dB on average, whereas the image index of the method we proposed is about 35 dB. Specifically, the proposed method achieved an average PSNR improvement of 1.9 dB.

This method also achieves good results in biometric recognition experiments. We have slightly interfered with the human eye area, so there is no doubt that the similarity around the eyes before and after image interference is extremely high. But for the whole image, we need to further compare the similarity before and after anonymity. As shown in Figure 12, the proposed method has obvious advantages on the MICHEI dataset. However, for the Face dataset, the overall cosine value is relatively lower. It's also because it is less anonymous.

As shown in Figure 12, the cosine similarity of the proposed method is above 0.9 and 0.98 in the two datasets, respectively. This shows that the proposed method can achieve high anonymity with minimal interference. The low value of the MICHEI dataset may be related to the error of the image. The image error refers to the abnormal state of the object in the image, such as the object's eyes being closed or the light being too strong to recognize the human eye or face. Figure 13 illustrates several error images in the database.

Because of the limit of anonymous success, we discuss changes in the cosine similarity only on the MICHEI dataset. Specifically, six sensors of the three devices (Apple iPhone5 Unit 1, Apple iPhone5 Unit 2, and Samsung Galaxy S4) improved by an average of around 0.02 points.

Finally, we report the results of the periocular biometric identification experiment. The experimental results show that the PRNU anonymous image can retain the biometric utility of the image. As shown in Figure 14, the proposed method has higher recall and precision than the one proposed by Banerjee and Ross (2020). In addition, the recall starts to change after the threshold

Figure 11. Comparison chart before and after anonymity. (a) original image; (b) anonymous image.

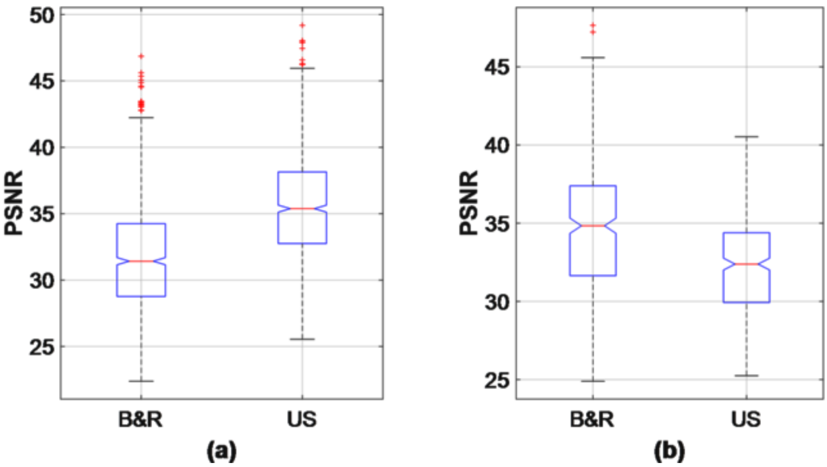


Figure 12. The comparison result of cosine similarity between our proposed method and the most advanced method proposed by Banerjee and Ross (2020) where the upper end of each of the 12 boxes is the maximum value of PSNR, the bottom is the minimum value, and the middle is the PSNR median. (A) the MICHEI dataset (B) the Face dataset.

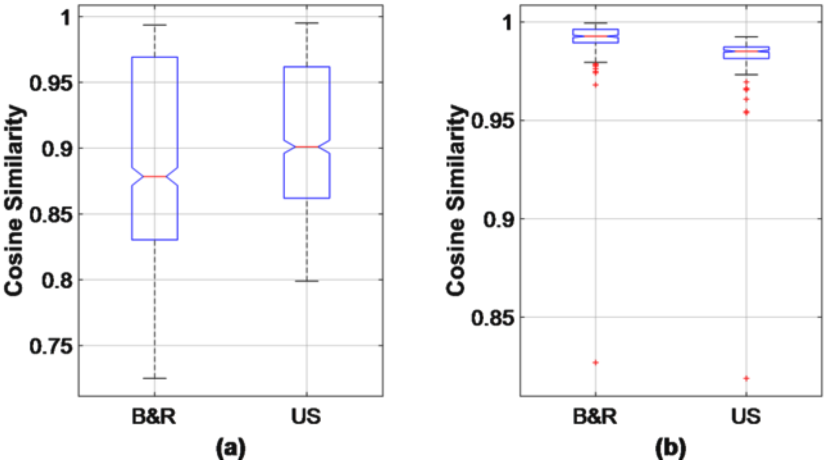
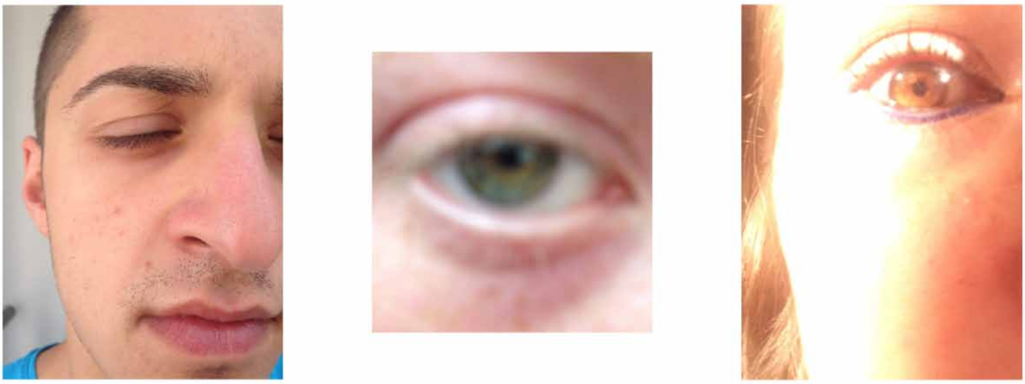


Figure 13. Some wrong images in MICHEI



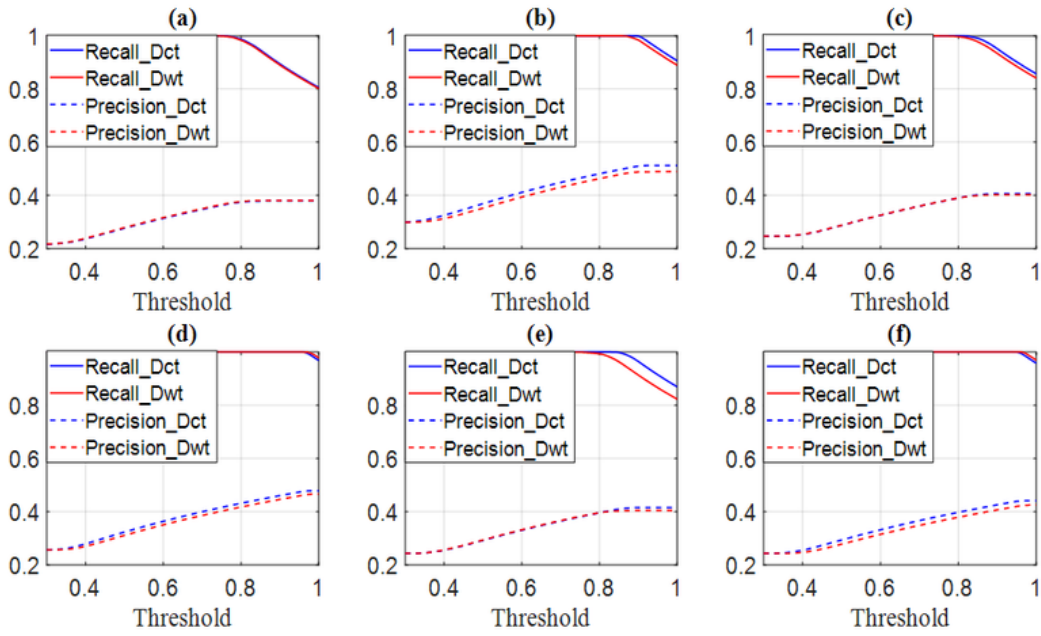
of 0.8, indicating that most samples of this model are correctly predicted. At the same time, it also reflects the overall low precision phenomenon. Aiming at this problem, we think that it is the reason of data polarization and centralization. There are also three times more negative samples than positive samples. The nature and quantity of data to make FP in Equation (8) are too large, which results in the overall low precision. However, the proposed method has improvement in recall and precision.

In summary, the proposed method not only ensures the success rate of anonymity but also has a higher PSNR value and similarity than the advanced method. Maintaining high image quality and high similarity between anonymous and original images is an important condition to maintain biological characteristics.

Computational Cost

In this section, we report the anonymity times for a single image for each device in the MICHEI dataset. The main frequency of the computer used in the experiment is 2.50 GHz, the memory is 8

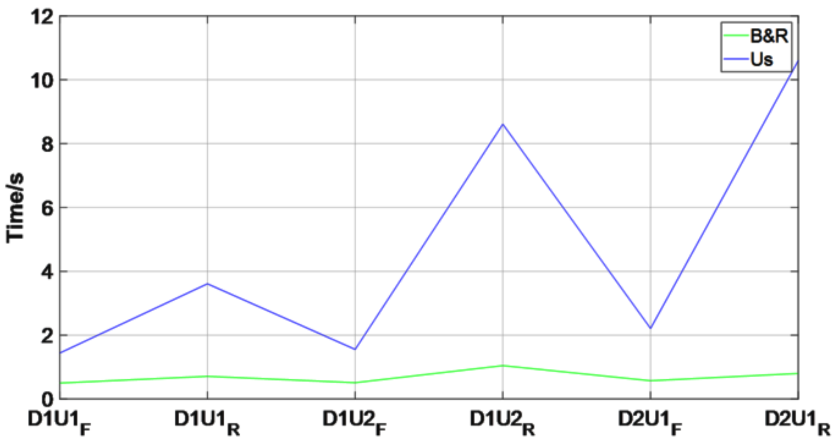
Figure 14. Comparison between the proposed method and the advanced method in terms of recall and precision. Sections (A)-(F) respectively represent the comparison results of six sensors in the MICHEI dataset.



GB, the operating systems are Microsoft Windows 10 Professional Edition and MATLAB 9.5. For the PRNU anonymous method based DCT, the parameters are set to the default configuration.

As shown in Figure 15, the calculation time based on the DCT method is lower and the processing speed is faster. The average processing time of each image can be as low as about 0.4 s. However, the method has poor PSNR and cosine similarity. In contrast, the proposed method has a long processing time and a positive correlation between the processing time and image size. When the image size is small, its processing time does not exceed 5 s. And it has better image quality compared with the DCT-based method. Therefore, the balance of all aspects of the proposed method is better.

Figure 15. Processing time per image for six sensors



FUTURE SCOPE AND APPLICATIONS

Privacy is one of the most important social and political issues (DeviPriya and Lingamgunta, 2020). Modern technologies, including the Internet of Things (IoT), multimedia, big data, and cloud computing, may provide a means to violate privacy (Tewari and Gupta, 2020). However, the fingerprint in the image-capturing device is unique to the individual. So, it can also indirectly harm individuals. The proposed method can achieve device anonymity without destroying biometrics, which has obvious advantages in solving this problem.

At present, most of the fingerprint suppression methods are driven by models. This mathematical model cannot accurately describe the complex imaging process, so it ignores the inherent defects of some device fingerprints. In recent years, deep learning technology has been widely used in image feature extraction, content-based image retrieval, and image content recognition. This method can greatly improve the image quality after fingerprint suppression. It will be the fingerprint technology research of the future development direction.

CONCLUSION

A new algorithm is designed to perturb biometric images to (a) obtain higher image quality while suppressing the association with the source sensor device and (b) ensure that the matching of images is not affected and the pass rate is higher. In this method, PRNU is anonymized by discrete wavelet transform and constant modulation of transform coefficients. In the case of biometric recognition, the proposed method performs different processing on different regions of the image. In the experiment, we considered images of faces taken from the front and back cameras of different smartphones. Experimental results show that PRNU is anonymized successfully. Compared with the prior art, the PSNR and cosine similarity of the proposed method are separately improved by about 1.9 dB and 0.02 points on average.

Future work will consider data from many sensors to evaluate the proposed algorithm. In addition, the effects of different denoising and PRNU estimation algorithms will be evaluated to investigate the robustness of the proposed method.

ACKNOWLEDGMENT

Many thanks to the reviewers for their helpful and constructive comments that have greatly improved this paper.

FUNDING STATEMENT

This research was funded by the National Natural Science Foundation of China (61872203 and 61802212), the Shandong Provincial Natural Science Foundation (ZR2022LZH011, ZR2020MF054, and ZR2019BF017), Major Scientific and Technological Innovation Projects of Shandong Province (2019JZZY020127, 2019JZZY010132, and 2019JZZY010201), Jinan City “20 universities” Funding Projects Introducing Innovation Team Program (20228016 and 2019GXRC031), Plan of Youth Innovation Team Development of colleges and universities in Shandong Province (SD2019-161), and the Project of Shandong Province Higher Educational Science and Technology Program (J18KA331).

REFERENCES

Banerjee, S., Mirjalili, V., & Ross, A. (2019). Spoofing PRNU patterns of iris sensors while preserving iris recognition. In *Proceedings of the 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, (pp. 1–10). IEEE doi:10.1109/ISBA.2019.8778483

Banerjee, S., & Ross, A. (2019). Smartphone camera de-identification while preserving biometric utility. In *Proceedings of the 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, (pp.1-10). IEEE. doi:10.1109/BTAS46853.2019.9185996

Bayram, S., Sencar, H. T., & Memon, N. D. (2013). Seam-carving based anonymization against image & video source attribution. In *Proceedings of the 2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP)*, (pp. 272-277). . IEEE. doi:10.1109/MMSP.2013.6659300

Bhme, R., & Kirchner, M. (2013). Counter-Forensics: Attacking Image Forensics. In H. Sencar & N. Memon (Eds.), *Digital Image Forensics*. Springer. doi:10.1007/978-1-4614-0757-7_12

Bonettini, N., Bondi, L., Güera, D., Mandelli, S., Bestagini, P., Tubaro, S., & Delp, E. J. (2018). Fooling PRNU-based detectors through convolutional neural networks. In *Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO)*, (pp. 957-961). IEEE. doi:10.23919/EUSIPCO.2018.8553596

Chen, M., Fridrich, J. J., Goljan, M., & Lukás, J. (2008). Determining image origin and integrity using sensor noise. *IEEE Transactions on Information Forensics and Security*, *3*(1), 74–90. doi:10.1109/TIFS.2007.916285

DeviPriya, K., & Lingamgunta, S. (2020). Multifactor two-way hash-based authentication in cloud computing. [IJAC]. *International Journal of Cloud Applications and Computing*, *10*(2), 56–76. doi:10.4018/IJCAC.2020040104

Dirik, A. E., Sencar, H. T., & Memon, N. D. (2014). Analysis of seam-carving-based anonymization of images against PRNU noise pattern-based source attribution. *IEEE Transactions on Information Forensics and Security*, *9*(12), 2277–2290. doi:10.1109/TIFS.2014.2361200

Galdi, C., Nappi, M., & Dugelay, J.-L. (2016). Multimodal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity. *Pattern Recognition Letters*, *82*(2), 144–153. doi:10.1016/j.patrec.2015.09.009

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition supplementary materials. In *Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (pp. 770-778). IEEE. doi:10.1109/CVPR.2016.90

Hernandez-Diaz, K., Alonso-Fernandez, F., & Bigün, J. (2018). Periocular recognition using CNN features off-the-shelf. In *Proceedings of the 2018 International Conference of the Biometrics Special Interest Group (BIOSIG)*, (pp. 1-5). IEEE.

Ju, X. (2020). An overview of face manipulation detection. *Journal of Cyber Security*, *2*(4), 197–207. doi:10.32604/jcs.2020.014310

Karakücük, A., & Dirik, A. E. (2015). Adaptive photo-response non-uniformity noise removal against image source attribution. *Digital Investigation*, *12*, 66–76. doi:10.1016/j.diin.2015.01.017

Kornblith, S., Shlens, J., & Le, Q. V. (2018). *Do better ImageNet models transfer better?* ArXiv. doi:10.48550/arXiv.1805.08974

Li, J., Lv, Y., Ma, B., Yang, M., & Zheng, Y. (2020). Video source identification algorithm based on 3D geometric transformation. *Computer Systems Science and Engineering*, *35*(6), 513–521. doi:10.32604/csse.2020.35.513

Li, T., Wang, L., Chen, Y., Ren, Y., & Xia, J. (2019). A face recognition algorithm based on LBP-EHMM. *Journal of Artificial Intelligence*, *1*(2), 59–68.

Liu, X., & Chen, X. (2020). A survey of GAN-generated fake faces detection method based on deep learning. *Journal of Information Hiding and Privacy Protection*, *2*(2), 87–94. doi:10.32604/jihpp.2020.09839

López, R. R., Orozco, A., & Villalba, L. (2020). Compression effects and scene details on the source camera identification of digital videos. *Expert Systems with Applications*, *170*, 114515. doi:10.1016/j.eswa.2020.114515

Lukas, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, *1*(2), 205–214. doi:10.1109/TIFS.2006.873602

Ma, B., Hu, Y., Li, J., Wang, C., & Zheng, Y. (2021). PRNU extraction from stabilized video: A patch maybe better than a bunch. *Computer Systems Science and Engineering*, *36*(1), 189–200. doi:10.32604/csse.2021.014138

Mandelli, S., Cozzolino, D., Bestagini, P., Verdoliva, L., & Tubaro, S. (2020). CNN-based fast source device identification. *IEEE Signal Processing Letters*, *27*, 1285–1289. doi:10.1109/LSP.2020.3008855

Marsico, M. D., Nappi, M., Narducci, F., & Proença, H. (2018). Insights into the results of MICHE I—Mobile iris challenge evaluation. *Pattern Recognition*, *74*, 286–304. doi:10.1016/j.patcog.2017.08.028

Narang, A., Gupta, D., & Kaur, A. (2020). Biometrics-based un-locker to enhance cloud security systems. [IJCAC]. *International Journal of Cloud Applications and Computing*, *10*(4), 1–12. doi:10.4018/IJCAC.2020100101

Newton, E. M., Sweeney, L., & Malin, B. (2005). Preserving privacy by de-identifying face images. *IEEE Transactions on Knowledge and Data Engineering*, *17*(2), 232–243. doi:10.1109/TKDE.2005.32

Picetti, F., Mandelli, S., Bestagini, P., Lipari, V., & Tubaro, S. (2022). DIPPAS: A deep image prior PRNU anonymization scheme. *EURASIP Journal on Information Security*, *2*(1), 2. Advance online publication. doi:10.1186/s13635-022-00128-7

Taspinar, S., Mohanty, M., & Memon, N. (2020). Camera identification of multi-format devices. *Pattern Recognition Letters*, *140*, 288–294. doi:10.1016/j.patrec.2020.10.010

Tewari, A., & Gupta, B. B. (2020). Secure timestamp-based mutual authentication protocol for IoT devices using RFID tags. *International Journal on Semantic Web and Information Systems*, *16*(3), 20–34. doi:10.4018/IJSWIS.2020070102

Zeng, H., Chen, J., Kang, X., & Zeng, W. (2015). Removing camera fingerprint to disguise photograph source. In *Proceedings of the 2015 IEEE International Conference on Image Processing*, (pp. 1687-1691). IEEE. doi:10.1109/ICIP.2015.7351088

Zhang, M., Zeng, K., & Wang, J. (2020). A survey on face anti-spoofing algorithms. *Journal of Information Hiding and Privacy Protection*, *2*(1), 21–34. doi:10.32604/jihpp.2020.010467

Jian Li is currently an associated professor with the School of Cyber Security, Qilu University of Technology, Jinan, China. He received the B.S. and M.S. degrees from Shandong University, Shandong, China, in 2004 and 2007, respectively, and the Ph.D. degree from Sun Yat-sen University, Guangdong, China, in 2011, all in computer science. His research interests are information hiding and forensics.