

A Novel Algorithm for Image Copy-move Forgery Detection and Localization based on SVD and Projection Data

Feng Liu^{1,2,*} and Hao Feng¹

1 College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310014, China

*2 Ningbo Institute of Technology, Zhejiang University, Ningbo, 315100, China
lf_nit@sina.com*

Abstract

With the widespread use of powerful image editing tools, the demand for identifying the authenticity of an image is much increased. Copy-move forgery is one of the most common and immediate tampering attacks, and is one type of image forgery where one region of an image is copied to another region in an attempt to cover some potentially important features. In this paper a Novel approach is presented for image copy-move forgery detection and localization based on SVD and Projection Data. Experiment results demonstrate that our proposed algorithm can effectively detect multiple copy-move forgery and precisely locate the duplicated regions, even when an image was distorted by Gaussian blurring, JPEG compression and their mixed operations.

Keywords: *Digital image forgery; copy-move forgery; SVD; Projection Data*

1. Introduction

With the development of computer technology, image tampering operation becomes easy and difficult to perceive. [1] A number of powerful image editing softwares have been developed, amidst which Adobe Photoshop might be the most popular one. The content of a digital image can be easily doctored with the help of image editing softwares. When the counterfeit images are used for vicious purpose, it may result in inestimable loss. Therefore, developing techniques to verify the authenticity and integrity of digital images become very imperative, which is one of the primary goals in image forensic. Image forensic aims at identifying the evidence of forgeries, whose primary mission is to reinforce the credibility of digital images. In contrast to the watermarking-based authentication approaches, image forensic can accomplish blind authentications without referring to any auxiliary information such as watermark [2] or signature. After nearly a decade of developments, image forensic has grown from infancy to maturity, and a number of algorithms have been proposed to cope with diverse forms of forgeries.

In this paper, we focus on the detection of copy-move that is the most common image tampering technique used due to its simplicity and effectiveness, in which parts of the original image is copied, moved to a desired location and pasted. This is usually done in order to hide certain details or to duplicate certain aspects of an image. Textured regions are used as ideal parts for copy-move forgery, since textured areas have similar color and noise variation properties to that of the image which are unperceivable for human eye looking for inconsistencies in image statistical properties. Blurring is usually used along the border of

* Corresponding Author

the modified region to lessen the effect of irregularities between the original and pasted region.

In the last decade, many passive detection schemes for copy-move forgery have been proposed. Fridrich [3] first analyzed the exhaustive search and then proposed a block matching detection scheme based on discrete cosine transform (DCT) which is one of the landmark methods for copy-move forgery detection. Popescu [4] proposed a similar method which used principal component analysis (PCA) instead of DCT. The accuracy of the method is good except for small block sizes and low SNR. Luo [5] extracted color features as well as special intensity ratio to represent a block characteristics vector. A different approach was presented by Kang [6] in which the features were represented by the singular value decomposition (SVD). Bayram [7] applied Fourier-Mellin transform (FMT) to each block and FMT values were finally projected to one dimension to form the feature vector. Mahdian [8] used a method based on blur moment invariants to locate the forgery regions. Li [9] extracted the features of the circular blocks using rotation invariant uniform local binary patterns. Lynch [10] proposed an efficient expanding block algorithm primarily using direct block comparison instead of indirect comparisons based on block features. Almost all the methods mentioned above are block-based which attempt to find an effective and robust representation of each block, moreover, they are expected to be insensitive to common post-processing operations including additive white Gaussian noise (AWGN), Gaussian blurring and JPEG compression.

Unlike block-based methods, keypoint-based methods do not divide the image into blocks to extract the features; instead, the features are extracted from the whole image. This approach can be accomplished by using methods such as the scale-invariant feature transform (SIFT) and speeded up robust features (SURF). Such techniques are used to extract distinctive local features in the image and to produce key-point descriptors that present those features. Those feature vectors/descriptors are invariant to rotation, translation, and scaling, are partially invariant to illumination changes and are robust to local geometric distortion [11, 12]. The first attempt to utilize the SIFT was made by Huang *et al.* [13]. In their algorithm, only the matching of SIFT key-points can be performed, by means of the best-bin-first nearest-neighbor identification. Ardizzone *et al.* [14] adopted SIFT to detect multiple copies in forged images. However, SIFT-based scheme still has a limitation on detection performance since it is only possible to extract the keypoints from peculiar points of the image and not robust to some post-processing operations like blurring and flipping based on our experimental results. Shivakumar [15] proposed another keypoint-based method which used speeded up robust features (SURF). Recently, Chen [16] developed a method by extracting Harris corner points as keypoints and employing step sector statistics to represent the small circle image region around each Harris point. The main drawback of most keypoint-based methods is that copied regions are often only sparsely covered by matched keypoints. Thus they do not provide the exact extent and location of the detected duplicated region, but only displays the matched keypoints. Furthermore, if the copied region exhibits little structure, it may happen that the region is completely missed [17].

In this paper, we develop an Novel and effective detection algorithm based on SVD and Projection Data whose framework is based on expanding block [10]. A series of experiments conducted on challenging realistic forgery images demonstrate our method can not only effectively detect multiple copy-move forgery and precisely locate the duplicated regions, but also has stronger robustness to common post-processing attacks such as Gaussian blurring, additive white Gaussian noise, JPEG compression and their mixed operations.

The rest of the paper is organized as follows. The basic theory of the Proposed Algorithm is given in Section 2. In Section 3, the proposed forgery detection method is described in

detail. The experimental results are given and the corresponding analysis is discussed in Section 4. The conclusion is drawn in Section 5.

2. The Basic Theory

2.1. Singular Value Decomposition

One of the basic and most important tools of modern numerical analysis, particularly numerical linear algebra, is the singular value decomposition. The SVD was established for real square matrices in the 1870's by Beltrami and Jordan. Singular value decomposition (SVD) is a matrix factorization and has three properties, namely, stability, scaling property and rotation invariance, which represents algebraic and geometric invariant properties of an image. SVD has been used in a large amount of fields such as signal processing, data compression and pattern analysis. The basic theory of SVD is as follows:

Let $A \in R_r^{m \times n}$. Then there exist orthogonal matrices $U \in R^{m \times m}$ and $V \in R^{n \times n}$ such that:

$$A = U \Sigma V^T, \Sigma \in R^{m \times n} \quad 2-1$$

where
$$\Sigma = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix}$$

and $S = \text{diag}(\sigma_1, L, \sigma_r)$ with $\sigma_1 \geq L \geq \sigma_r > 0$

SVD is not only an important tool for exploratory data analysis, dimensionality reduction and data compression, but also a method for noise reduction. The singular values are unique for a matrix, which form a steady representation of image blocks. In Σ , There are only a few large singular values dominate for most natural images while all the other singular values are quite small. It can be drawn that the relatively small singular values are sensitive to noise while the largest singular value contains most energy of each image block and has a good stability even when images suffer from minor distortions. This is the property of SVD of which our algorithm takes advantage.

2.2. The Projection Data

In the field of image matching and image retrieval, the projection data as image features for matching and retrieval has many successful applications, such as Offline character recognize, Face recognition and License plate recognition. In these applications, the image features are the projection data of the horizontal direction and the vertical direction. The projection curve of the horizontal direction and the vertical direction reflects the gray feature of the horizontal and vertical direction fully, can significantly reduce the image dimension and the computation complexity.

In our proposed algorithm, we apply the projection data of the image as the features to the image forensics. Suppose the size of a small image block is $n \times n$, the gray function is $f(x, y)$, the projection of the horizontal direction is one dimensional vector $H(i)$, the projection of the vertical direction is one dimensional vector $V(i)$.

$$H(i) = \sum_{k=1}^n f(i, k), 0 \leq i \leq n \quad 2-2$$

$$V(i) = \sum_{k=1}^n f(k, j), 0 \leq j \leq n \quad 2-3$$

Then, in order to reduce the dimension and the computation complexity, a new two dimensional matrix $M(u, v)$ is generated using $H(i)$ and $V(i)$.

For example:

Let $n = 8$, the new matrix $M(u, v)$ is

$$\begin{pmatrix} H(1) & H(2) & H(3) & H(4) \\ H(5) & H(6) & H(7) & H(8) \\ V(1) & V(2) & V(3) & V(4) \\ V(5) & V(6) & V(7) & V(8) \end{pmatrix} \quad 2-4$$

Let $n = 16$, the new matrix $M(u, v)$ is

$$\begin{pmatrix} H(1) & H(2) & H(3) & H(4) & H(5) & H(6) \\ H(7) & H(8) & H(9) & H(10) & H(11) & H(12) \\ H(13) & H(14) & H(15) & H(16) & V(1) & V(2) \\ V(3) & V(4) & V(5) & V(6) & V(7) & V(8) \\ V(9) & V(10) & V(11) & V(12) & V(13) & V(14) \\ V(15) & V(16) & 0 & 0 & 0 & 0 \end{pmatrix} \quad 2-5$$

Last, apply SVD to the $M(u, v)$ and get the $\Sigma = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix}$, $S = \text{diag}(\sigma_1, \dots, \sigma_r)$ with $\sigma_1 \geq \dots \geq \sigma_r > 0$

2.3. The Method of Expanding Block

In [10], the author proposed a method of expanding block. The proposed method primarily divides an image into N_b small overlapping blocks just like in the usual block method. However, the approach to comparing the blocks is different. Because many of the blocks are obviously different, so the blocks do not need to be compared against each other. A dominant feature is computed for each block. If the dominant feature differs vastly between blocks, there is no need for comparison. Blocks are grouped together according to their dominant features. The blocks are sorted by dominant feature and placed evenly (or as evenly as possible) into G groups, each of which contains the blocks with a similar dominant feature. The first and last blocks in a group will also have a similar dominant feature to the blocks in the previous and next groups, respectively. To remedy this problem, we create G buckets so that the i th bucket contains the blocks from group i , $i - 1$, and group $i + 1$. Each block will be placed into 3 buckets (except the blocks that are in the first and last groups which will only be placed into 2 buckets). Figure 1 illustrates an example of how blocks are sorted and placed into buckets. At last, blocks are compared only against other blocks in the same bucket. The comparisons are conducted using the dominant features.

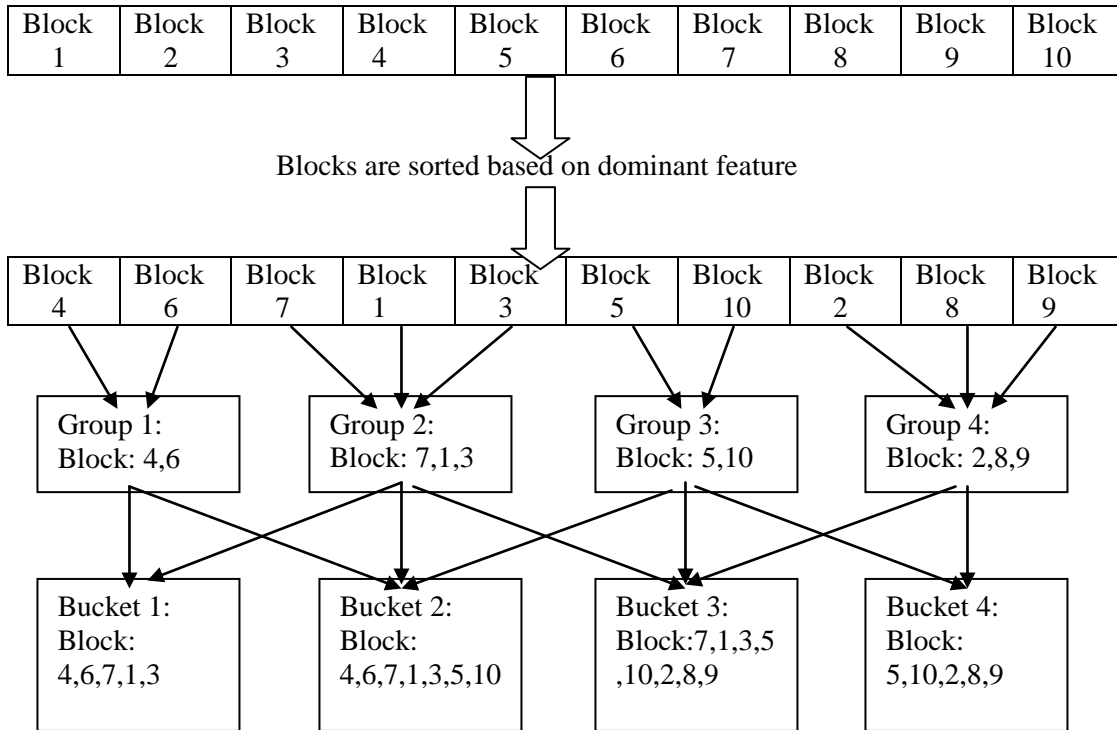


Figure 1. An Example of How Blocks are Sorted and Placed into Buckets

3. The Proposed Algorithm

Because of the nature of copy-move forgery, there must be at least a pair of similar regions in a tampered image, which is the basis of all copy_move forgery detection algorithms. A natural image, on the contrary, is unlikely to have two large similar regions except for the images that have a large area of smooth region, such as blue sky or green grassland in the image. Here we assume that the duplicated regions are non-overlapping. The task of the detecting method is to determine whether an image contains duplicated regions. Since the shape and size of the regions are unknown, it is definitely computationally impossible to try to examine every possible pairs of region with different shape and size. The key step is to extract some appropriate and robust features from each block in order to implement an effective detection. Therefore, a good feature can not only represent the whole block, but also has the robustness of common post-processing operations, and what is more, make the detection algorithm have lower computational complexity.

The proposed algorithm based on SVD and Projection Data is presented below.

Assume that the suspicious image is a gray image. If it is a color image, it is first converted to a grayscale image using the standard formula:

$$Y = 0.299R + 0.587G + 0.114B$$

Where R, G, B are three channels of the input color image, Y is its luminance component.

1. Divide an image I into small overlapping blocks of size 16×16 .
2. Perform SVD to each block and get matrices U, S and V for each block, acquire the $S(1,1)$ of each S matrix as the dominant feature.
3. Sort the blocks based on the dominant feature.

4. From the sorted blocks, place the blocks evenly into numBuckets groups.
5. Create numBuckets buckets. Place the blocks from groups $i - 1$, i , and $i + 1$ into bucket i .
6. Process every bucket as follows:
 - a. Suppose there are N blocks in the bucket. Construct an $N \times N$ matrix called the connection matrix. It denotes which blocks match each other. Initially, set the connection matrix to all ones so that all blocks match each other.
 - b. If two blocks are less than blockSize pixels away, then the two blocks overlap. Set the connection matrix to 0 for these blocks.
 - c. Like 2.2, compute the projection of the horizontal direction $H(i)$ and the projection of the vertical direction $V(i)$ of each block in the bucket. Then using the $H(i)$ and $V(i)$ to create a new matrix $M_i(u, v)$ like 2-5.
 - d. Apply SVD to $M_i(u, v)$ and get the $S_{M_i} = (\sigma_{i1}, L, \sigma_{i6})$ as the feature vector of each block in the bucket. Compute the distance of every two blocks through the feature vector in the bucket according to the formula:
$$d = \sqrt{\sum_{n=1}^6 (\sigma_{in} - \sigma_{jn})^2}$$
.
 - e. If the distance d of the two blocks is less than pvalThreshold, then set the connection in the connection matrix to 0 for these blocks.
7. For each bucket, If the connection matrix has a row of zeros, then the block corresponding to this row is not connected to any other block in the bucket. Remove this block from the bucket.
8. From the remaining blocks in the buckets, compute the total area. If the total area is less than minArea, then discard the remaining blocks; otherwise, the remaining blocks are assumed to be part of the duplicated region.
 - numBuckets: the number of buckets used to compare blocks
 - pvalThreshold : a value used for the distance threshold for comparing blocks
 - minArea: a value denoting the minimum area of the duplicated region.

4. Experiment Results and Analysis

This section is divided into three subsections. The first will introduce the evaluation criteria. The second subsection will introduce the visual result of the proposed algorithms. Third subsection will compare the algorithm with other existing algorithms. All measurements are performed on a Lenovo laptop with a 2.1 GHz Intel Pentium processor and 4 GB of RAM.

4.1. Evaluation Criteria

For practical applications, the most important aspect of a detection method is the ability to distinguish tampered and original images. However, the power to correctly locate the tampered region is also significant, which gives the strong evidence to expose digital forgeries. Thus, we evaluate the performance of our algorithm at image level, where we focus on whether the fact that an image has been tampered or not can be detected; at pixel level, where we evaluate how accurately can tampered regions be identified.

At image level, we keep a record of some important measures which are the number of correctly detected forged images T_p , the number of images that have been erroneously

detected as forged r , and the falsely missed forged images F_N . From these we compute the measures Precision, p and Recall, r which are defined as follows [17]:

$$p = \frac{T_p}{T_p + F_p} \quad \text{and} \quad r = \frac{T_p}{T_p + F_N} \quad 2-7$$

Precision denotes the probability that a detected forgery is truly a forgery; while Recall shows the probability that a forged image is detected.

At pixel level, we adopt two quantitative measures to evaluate the performance of the proposed algorithm. Denote ψ_S, ψ_T as pixels of original region and forgery region in original image respectively, and $\dot{\psi}_S, \dot{\psi}_T$ as pixels of original region and forgery region in detected result image respectively. From these we compute the detection accuracy rate DAR and the false positive rate FPR . They are defined as follow:

$$DAR = \frac{|\psi_S \cap \dot{\psi}_S| + |\psi_T \cap \dot{\psi}_T|}{|\psi_S| + |\psi_T|} \quad 2-8$$

$$FPR = \frac{|\dot{\psi}_S - \psi_S| + |\dot{\psi}_T - \psi_T|}{|\dot{\psi}_S| + |\dot{\psi}_T|} \quad 2-9$$

Where ‘|’ means the area of region. ‘ \cap ’ means the intersection of two regions and ‘ \sim ’ means the difference of two regions. In this sense DAR indicates the performance of algorithm correctly locating pixels of copy-move regions in the tampered image, while FPR reflects the percentage of pixels which are not contained in duplicated region but included by the implemented method. That is, two parameters indicate how precisely our algorithm can locate copy-move regions. The more DAR is close to 1 and FPR is close to 0, the more precise the method would be.

4.2. The Visual Results

The images shown in Figure 2 and Figure 3 were the results of detecting tampered images without any distort operations. Each image was composed of three images: original image, tampered image and map image from left to right. From the visual result. Our algorithm could detect all the cases precisely. It was noted that Figure 3 and Figure 4 also indicated that the algorithm could process some images having one and multiple regions in visual sense.

4.3. Comparison with Other Algorithms

In this section, the performance of our proposed algorithm (labeled SPD) is compared with other algorithms, which are based on the sliding block algorithm using nearest neighbor comparison: principal component analysis (labeled PCA). Every comparison will include the measures Precision, p which denotes the probability that a detected forgery is truly a forgery and Recall, r which shows the probability that a forged image is detected, DAR indicates the performance of algorithm correctly locating pixels of copy-move regions in the tampered image, FPR reflects the percentage of pixels which are not contained in duplicated region but included by the implemented method .

In the first set of experiments, a separate set of 100 grayscale images of size 256×256 was used for the comparisons. The block size was set to 16. The copied region was assumed to be at least 24×24 , numBuckets was set to 2048 and pvalThreshold was set to 3. To test the algorithms with forgeries, a square of random size from 24×24 to 64×64 was copied and pasted into a non-overlapping random location within the same image. This was done 10 times for every image for a total of 1000 forged images (10 different forgeries for each of 100 images) and 100 non-forged images.

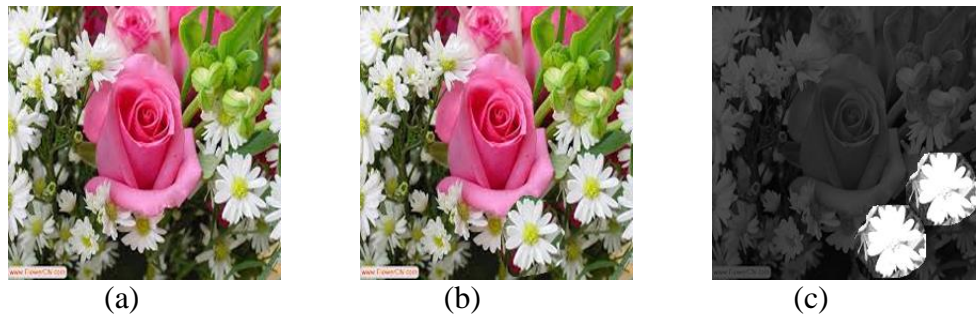


Figure 2. (a) The Original Image (b) The Forged Image with a Copied Region (c) The Map Image

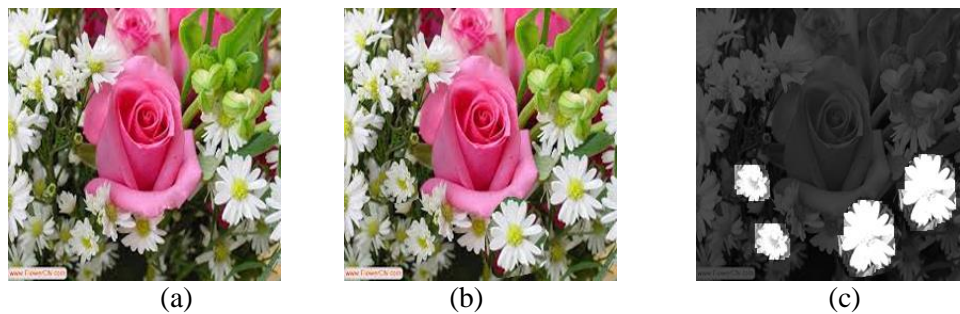


Figure 3. (a)The Original Image (b) The Forged Image with Two Copied Regions (c) the Map Image

4.3.1. Without any Additional Modifications: Figure 4 shows an example of a copy-move forgery and the results from two detection methods. From the visual results, we can see that the proposed algorithm get better effect than the PCA method. The proposed algorithm is able to correctly identify the forged with no mistakes. Table 1 shows the performance time of different methods. It is able to see that the performance time of SPD is faster than PCA.

Table 2 shows the test of a basic comparison of the methods involving the original images and the forged images without any additional modifications. The proposed algorithm has the *DAR* with 0.996 similar to the PCA algorithm' *DAR* with 0.998. But the *FPR* of PCA algorithm with 0.012 is by far larger than the *FPR* of the proposed algorithm with 0.003.

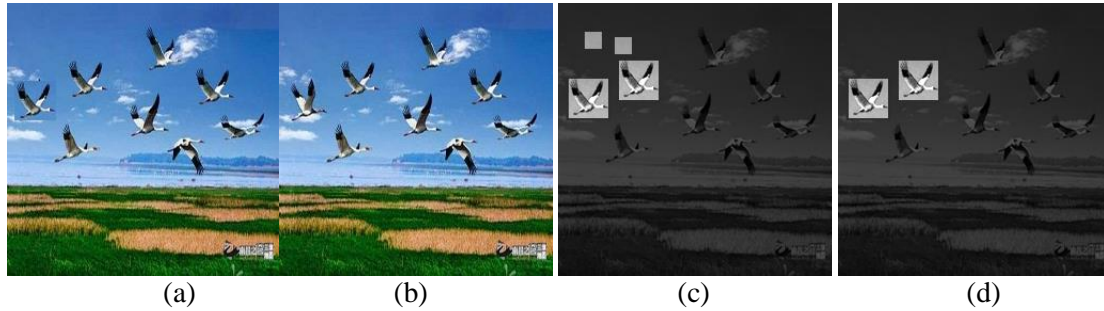


Figure 4. (a)The Original Image (b) the Forged Image (c)PCA Copy Move Detection (d) the SPD Copy Move Detection

Table 1. The Performance Time of Different Methods

method	PCA	SPD
seconds	28.00	13.10

Table 2. Comparison of the Methods where the Forged Imaged without any Additional Modifications

	PCA	SPD
p	1	1
r	1	1
DAR	0.998	0.996
FPR	0.012	0.003

Table 3. Comparison of the Methods under JPEG Compression

	1		0.95		0.9		0.85	
	PCA	SPD	PCA	SPD	PCA	SPD	PCA	SPD
DAR	0.632	0.910	0.376	0.798	0.278	0.689	0.124	0.118
FPR	0.231	0.102	0.442	0.210	0.578	0.256	0.706	0.698

Table 4. Comparison of Methods with Different Gaussian Blurring

	$\omega = 3, \sigma = 0.5$		$\omega = 3, \sigma = 1$		$\omega = 3, \sigma = 2$		$\omega = 3, \sigma = 3$	
	PCA	SPD	PCA	SPD	PCA	SPD	PCA	SPD
DAR	0.984	0.982	0.934	0.943	0.864	0.887	0.793	0.838
FPR	0.011	0.008	0.034	0.032	0.064	0.053	0.092	0.087

4.3.2. JPEG Compression: This set of tests will investigate the performance of the proposed algorithm under JPEG compression. In Table 3, the compression ratios used are 1, 0.95, 0.9 and 0.85, where compression ratio is the compressed file size divided by the original file size.

In Table 3, we can see that the performance evaluations of SPD are better than the PCA at the compression ratios that are 1、0.95 and 0.9 respectively, which indicate that our method has the ability to locate tampered regions in the case of slight compression.

4.3.3. Gaussian Blurring: Table 4 shows the test for the effect of Gaussian blurring. The Gaussian blurring uses $\omega = 3$, and $\sigma = 0.5、1、2、3$.

In the case of Gaussian blurring, Table 4 indicates that the DAR value of the proposed method gains better performance than the PCA method, with $DAR > 0.83$, when the blurring radius increases. The FPR curve also gives a satisfactory result that our method has the lower FPR, even though with larger blurring radius $\sigma = 3$.

5. Conclusions

We have proposed a robust passive detection method for copy-move forgery which works in the absence of digital watermarks or signatures information. Compare with previous works, such as PCA methods, our algorithm used less features to represent each blocks, and was more effective. The experiment results show that the proposed algorithm could not only effectively detect multiple copy-move forgery and precisely locate the duplicated regions, but also has stronger robustness to Gaussian blurring, JPEG compression and their mixed operations. Thus, we believe our method could be useful in some areas of forensic science.

References

- [1] A. Ho, Y. Shi, H. Kim, M. Barni, W. Wang, J. Dong and T. Tan, "A survey of passive image tampering detection", *Digital Watermarking*, vol. 5703, Springer, Berlin/Heidelberg, (2009), pp. 308–322.
- [2] S. Katzenbeisser and F. Petitcolas, "Information Techniques for Steganography and Digital Watermarking", Artec House, (2000).
- [3] J. Fridrich, D. Soukalm and J. Lukas, "Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop", Cleveland, (2003), pp. 19–23.
- [4] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions", Tech. Rep. TR2004-515, Dartmouth College, (2004).
- [5] W. Luo, J. Huang and G. Qiu, "Robust detection of region-duplication forgery in digital images", in: *International Conference on Pattern Recognition*, vol. 4, (2006), pp. 746–749.
- [6] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", in: *Proceedings of International Conference on Computer Science and Software Engineering*, (2008), pp. 926–930.
- [7] S. Bayram, H. T. Sencar and N. Memon, "An efficient and robust method for detecting copy-move forgery", in: *IEEE International Conference on Acoustics, Speech and Signal Processing*, IEEE Press, New York, (2009).
- [8] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants", *Forensic Sci. Int.* vol. 171, (2007), pp. 180–189.
- [9] L. Li, S. Li and H. Zhu, "An efficient scheme for detecting copy-move forged images by local binary patterns", *J. Inf. Hiding Multimedia Signal Process.*, vol. 4, no. 1, (2013), pp. 46–56.
- [10] G. Lynch, F. Y. Shih and H. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection", *Inf. Sci.* vol. 239, (2013), pp. 253–265.
- [11] D. G. Lowe, "Object recognition from local scale-invariant features", in: *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2, (1999), pp. 1150–1157.
- [12] H. Bay, T. Tuytelaars and L. Van Gool, "SURF: speeded up robust features, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence).
- [13] H. Huang, W. Guo and Y. Zhang, "Detection of copy-move forgery in digital images using sift algorithm", in: *Proceedings – 2008 Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, PACIIA 2008, (2008), pp. 272–276.
- [14] E. Ardizzone, A. Bruno and G. Mazzola, "Detecting multiple copies in tampered images", in: *Proceedings – International Conference on Image Processing, ICIP*, (2011), pp. 2117–2120.

- [15] B. L. Shivakumar and S. Baboo, "Detection of region duplication forgery in digital images using SURF", Int. J. Comput. Sci. Issues, vol. 8, no. 4, (2011), pp. 199–205.
- [16] L. Chen, W. Lu, J. Ni, W. Sun and J. Huang, "Region duplication detection based on Harris corner points and step sector statistics", J. Vis. Comm. Image Representation, vol. 24, (2013), pp. 244–254.
- [17] V. Christlein, C. Riess and J. Jordan, *et al.*, "An evaluation of popular copy-move forgery detection approaches", IEEE Trans. Inf. Forensics Secur. vol. 7, no. 6, (2012), pp. 1841–1854.

Authors

Feng Liu is currently a Ph.D. student in the College of Information Engineer, Zhejiang University of Technology in China. His research focuses on image processing, multimedia watermarking and information forensics and he has published several papers in scholarly journals and international conferences in the above research areas.

Hao Feng is currently a professor in the College of Information Engineer, Zhejiang University of Technology in China. Professor Feng has published over 60 research papers in scholarly journals and international conferences. His main research interests include pattern recognition, artificial neural network and image processing.

