http://ansinet.com/itj

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (7): 1341-1345, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1341.1345


# Detection of Composite Images Based on Simgle Channel Blind Signal Separation

[1]Wei Wang, [1]Feng Zeng, [2]Xintao Duan and [1]Hongjun Li
[1]School of Electronics and Information, Nantong University, Nantong Jiangsu 226019, China
[2]School of Computer and Information Technology, Henan Normal University,
Xinxiang Henan 453007, China

**Abstract:** A common technique of photographic manipulation is the digital splicing combining two or more images into a single composite. However, many of the existing detection methods are limited to handle merely one type of splicing image. In this study, a novel method is proposed to detect the splicing by using Single Channel Blind Signal Separation (SCBSS). The mixing matrix can be constructed through the splicing definition in order to build a new SCBSS model. A new measure is developed to estimate the special binary matrix, which recover all source images. These images allow identifying the spliced region and the background region. The experiment results are promising and confirm the robustness of the proposed approach.

**Key words:** Passive image forensics, image composition, SCBSS, characteristics domain

## INTRODUCTION

With the development of sophisticated image editing tools and softwares, various types of digital forgeries can be easily created. One of the most common types of image forgeries is the image splicing. Over the past few years, many techniques have been developed to discover such splicing and compositing of images. Farid (2009a, b) roughly groups blind approaches for image splicing detection into four categories: (1) Pixel-based techniques, (2) Format-based techniques, (3) Camera-based techniques and (4) Physically based techniques. In the first group, unnatural correlations resulting (Popescu and Farid, 2005a) from the resampling process when tampering an image are identified and utilized as clues of forgery. As in the second categories, Farid (2009a) exploited properties of specific lossy compression schemes for digital forgery detection. This method detects whether a part of an image was initially compressed at a lower quality than the rest of the image. Methods belonging to the third approach are also introduced for forgery detection by exploiting artifacts introduced by the camera. By detecting the difference of color filter array (Popescu and Farid, 2005b), sensor noise (Chen *et al*., 2008) and camera response (Hsu and Chang, 2010), the inconsistency in altered images can be obtained. In the fourth group, several methods using physical rules detect anomalies of interaction between objects in the target scene. Johnson and Farid (2007) proposed to detect image splicing using inconsistency of lighting direction. Photometric consistency of illumination (Liu *et al*., 2011) in shadows is often a useful constraint for finding suspicious shadows. Composites of image are detected using the perspective constraint that the height ratio of two objects in an image should be different (Yao *et al*., 2012).

Each of the methods mentioned above are limited to handle merely specific kinds of tampering. Since many researchers pay attention to find new features or new approaches for splicing detection in the earlier research, but few is concerned on mathematical model and theoretical research. In this study, a novel method is proposed to detect the splicing by using Single Channel Blind Signal Separation (SCBSS). A new measure is developed to estimate the special binary matrix, which recover all source images. These images allow identifying the spliced region and the background region. The experiment results show the general effectiveness of this technique even if the images to be tested have been noised with different levels or compressed with a low quality factor.

## PROBLEM FORMULATION

According to the definition of spliced images, the mathematical model is described by the following Equation:

$$y(i,j) = A_0 \odot s_0(i,j) + A_1 \odot s_1(i,j) + \cdots + A_N \odot s_N(i,j) = A.s(i,j) \quad (1)$$

**Corresponding Author:** Feng Zeng, School of Electronics and Information, Nantong University, 226019, China

where, y(i, j) is the spliced image, ⊙ denotes Hadamard product, $s(i, j) = [s_0(i, j), s_1(i, j),..., s_N(i, j)]^T$ is the (1+N)×1 vector of source images, $A = [A_0, A_1,..., A_N]$ is the 1×(1+N) vector of mixing matrixes. Where the splicing matrixes $A_n$ are:

$$A_0 = \begin{cases} 1 & (i,j) \in U_0 \\ 0 & (i,j) \in U_1 \\ \vdots & \\ 0 & (i,j) \in U_N \end{cases}, A_1 = \begin{cases} 0 & (i,j) \in U_0 \\ 1 & (i,j) \in U_1 \\ \vdots & \\ 0 & (i,j) \in U_N \end{cases}, \cdots, A_N = \begin{cases} 0 & (i,j) \in U_0 \\ 0 & (i,j) \in U_1 \\ \vdots & \\ 1 & (i,j) \in U_N \end{cases}.$$

where, $U_0$, $U_1$,..., $U_N$ denote the activation region with $U_0 \cup U_1 \cup ... \cup U_N = U$ and $\forall n, m, U_n \cap U_m = \varnothing$.

In order to make a seamless and plausible spliced image in practice, applying post-processing is indispensable and inevitable. Furthermore, blur operation is one of the commonly used methods to conceal the traces of tampering. The blurred spliced image is modeled as:

$$\begin{aligned} y(i, j) = A_0 \odot s_0(i, j) + h_1(i, j) \otimes (A_1 \odot s_1(i, j)) + \\ \cdots + h_N(i, j) \otimes (A_N \odot s_N(i, j)) \end{aligned} \quad (2)$$

where, ⊗ denotes convolution operator, $h_n$ (i, j) is the blurring kernel, n = 1, 2,...N. In general, the blurring kernel size is much smaller than the spliced region. Neglecting some edge points, Eq. 2 is also equivalent written as:

$$\begin{aligned} y(i, j) &= A_0 \odot s_0(i, j) + A_1 \odot (h_1(i, j) \otimes s_1(i, j)) + \cdots + A_N \odot (h_N(i, j) \otimes s_N(i, j)) \\ &= A.\ s(i, j) \end{aligned} \quad (3)$$

where, $s(i, j) = [s_0(i, j), h_1(i, j) \otimes s_1(i, j), \cdots, h_N(i, j) \otimes s_N(i, j)]^T$ is the (1+N)×1 vector of source images, $A = [A_0, A_1,..., A_N]$ is the 1×(1+N) vector of mixing matrixes. Equation 1 and 3 are typical single channel mixture model.

## PROPOSED FORGERY DETECTION METHOD

This study proposed a method which can detect image forgeries by using SCBSS. Proper characteristics domain is first represented from the given image. Based on this characteristics domain, the mixing matrix can be estimated and all source image blocks can be recovered. These image blocks allow identifying the spliced region and the background region.

**Characteristics domain represents:** In general, the spliced region and the background region have different characteristics in a sense because they came form different original images. Taking the Characteristics Domain Transform (CDT), the spliced image can be represented as:

$$Y(\omega) = F[S_0(\omega), S_1(\omega), \cdots, S_N(\omega)] \quad (4)$$

where, Y, $S_0$, $S_1$,..., $S_N$ represent the characteristics domain transform of Y, $S_0$, $S_1$,..., $S_N$, respectively, ω denotes characteristics factor, F[.] denotes nonlinear mixed.

Form Eq. 4, obviously, Y(ω) is a global mixed. In other words, the characteristics, $S_0$, $S_1$,..., $S_N$ has not activation region as defined earlier. Our goal is to estimate these characteristics, $S_0$, $S_1$,..., $S_N$, then recovers the mixing matrixes A.

**Mixing matrix estimates:** In order to increase the robustness to the noise, the clustering algorithm is exploited to estimate the mixing matrixes $A_0$, $A_1$,..., $A_N$. The clustering criterion function is defined as:

$$d = \frac{1}{k} \sum_{u=1}^{k} \sum_{v=1}^{k} (Y_u - Y_v)^2 \quad (5)$$

where, d denotes euclidean distance, $Y_u$ and $Y_v$ are the 1×k vector of characteristic points. This metric is used to determine the clusters of the characteristic points. $Y_u$ and $Y_v$ will be amalgamated into same cluster when d is below a predetermined threshold τ. In this case, when all subsequent characteristic points are carried out in Eq. 5, the mixing matrixes A can be recovered using different clusters, making us able to identify the value 1 of the binary mixing matrix.

**Source image separates:** According to the mixing matrix recovered in the section III-B and defined in the section II, the left multiplication $A^T$ of (1) could be written as:

$$A^T.\ Y(i, j) = A^T.\ A.\ s(i, j) \quad (6)$$

$$\begin{aligned} \begin{bmatrix} A_0 \\ A_1 \\ \cdots \\ A_N \end{bmatrix} \cdot y(i, j) &= \begin{bmatrix} A_0 \\ A_1 \\ \cdots \\ A_N \end{bmatrix} \cdot [A_0, A_1, \cdots, A_N] \cdot \begin{bmatrix} s_0(i, j) \\ s_1(i, j) \\ \cdots \\ s_N(i, j) \end{bmatrix} \\ &= \begin{bmatrix} A_0 & 0 & \cdots & 0 \\ 0 & A_1 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & A_N \end{bmatrix} \cdot \begin{bmatrix} s_0(i, j) \\ s_1(i, j) \\ \cdots \\ s_N(i, j) \end{bmatrix} \\ &= \begin{bmatrix} A_0 \odot s_0(i, j) \\ A_1 \odot s_1(i, j) \\ \cdots \\ A_N \odot s_N(i, j) \end{bmatrix} \end{aligned} \quad (7)$$

From Eq. 7, the separated results are not the source images $s_0$, $s_1$,..., $s_N$, but the subblocks, making us able to identify the spliced regions and the background regions.

## EXPERIMENTAL RESULTS

In the first experiment, simulations are performed to show efficacy of the proposed method. Some examples of the detection for spliced regions are shown in below images. In Fig. 1, column (a) gives two JPEG spliced images, where the spliced regions and the background regions undergone compressed with JPEG quality factors 70, 89 and 55, 88 (from up to down), respectively. Column (b) in each figure shows the corresponding CDT image of the quality factors. The mixing matrixes A can be estimated using different clusters of characteristic points, as defined in section III-B. The background regions and the spliced regions are accurately separated by left multiplying $A^T$ method defined in section III-C, as shown in column (c) and (d). It is observed that the proposed method can correctly indentify fake objects with inconsistent JPEG quality factors even if there are close to each other.

In Fig. 2, column (a) gives two resampling spliced images, where the spliced regions undergone nearest neighbor interpolation with 1.25 and bilinear interpolation with 1.5 (from up to down), respectively. Column (b) gives the corresponding CDT image of the interpolation factors. Column (c) and (d) give the separation results. Form experimental results, the proposed algorithm can correctly detect forgery objects with inconsistent resampling factors.

Figure 3 gives the detection results of spliced images with different background noise levels. Column (a) gives two noisy spliced images, where the background regions and the spliced regions with different background noise levels $\sigma_1 = 10^{-6}$ and $\sigma_2 = 10^{-4}$, respectively. Column (b) gives the corresponding CDT image of double imnoise correlation. Column (c) and (d) are the separation results. Form experimental results, the spliced regions are almost completely separated.

In order to make a seamless and plausible spliced image in practice, applying post-processing is indispensable. Figure 4 gives the detection results of spliced images with undergone blurring. Column (a) are two blurring spliced images, where the spliced regions undergone Gaussian blur and Shape blur (from up to down), respectively. Column (b) gives the corresponding CDT image of douible blur correlation. Column (c) and (d) give the separation results.

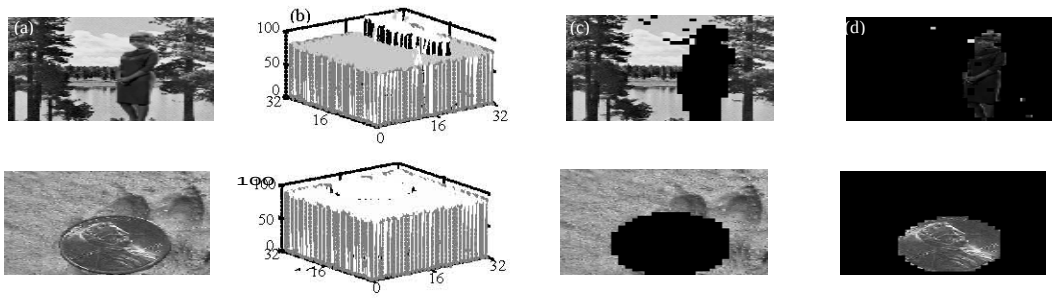


Fig. 1(a-d): JPEG spliced images and their separation results, (a) JPEG spliced images, (b) Characteristics domains constructed by quality factors and (c-d) Separation results

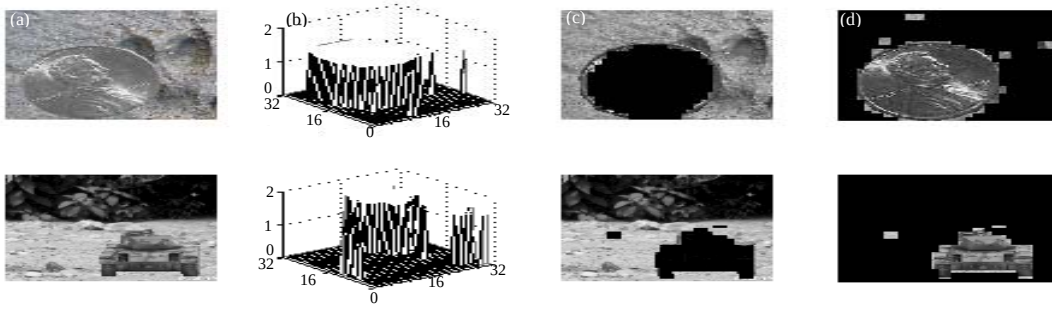


Fig. 2(a-d): Interpolated spliced images and their separation results, (a) Interpolated spliced images, (b) Characteristics domains constructed by interpolation factors and (c-d) Separation results

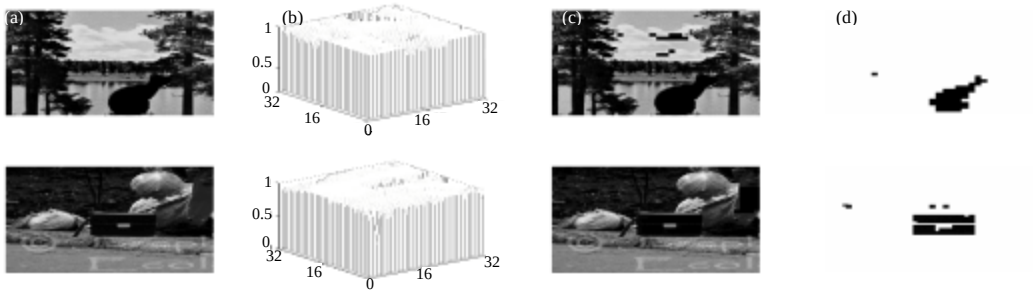


Fig. 3(a-d): Noisy spliced images and their separation results, (a) Noisy spliced images, (b) Characteristics domains constructed by double imnoise correlation coefficients and (c-d) Separation results

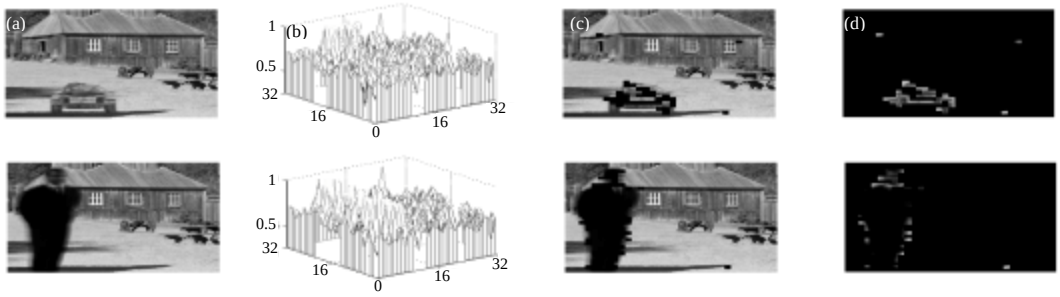


Fig. 4(a-d): Blurring spliced images and their separation results, (a) Blurring spliced images, (b) Characteristics domains constructed by double blur correlation coefficients and (c-d) Separation results

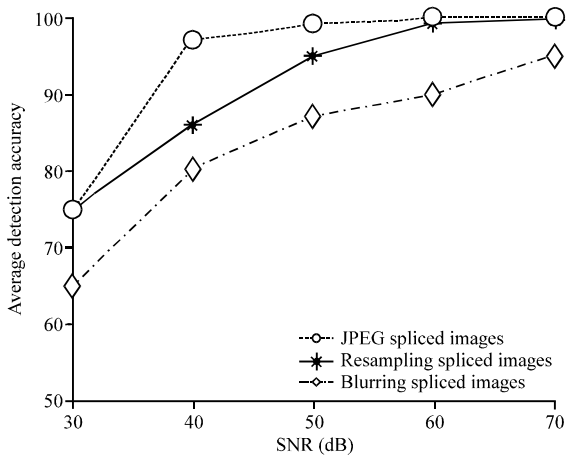


Fig. 5: Detection accuracy as a function of SNR

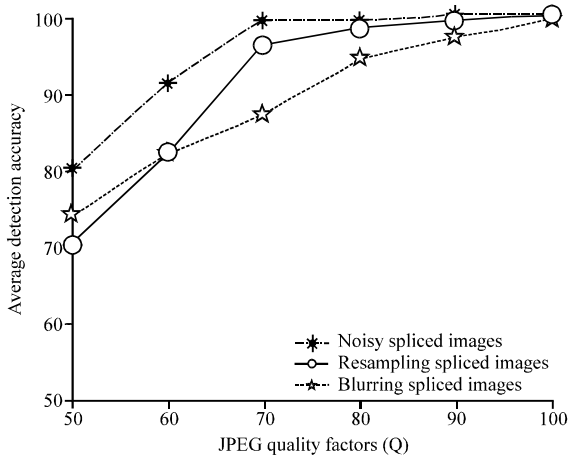


Fig. 6: Detection accuracy as a function of JPEG compression

It is observed that the proposed algorithm can correctly detect fake objects with inconsistent blurs.

In the second experiment, the robustness of the proposed approach was also tested. Figure 5 compares the performance of our algorithm on spliced images with different noise levels. The comparison shows that the proposed algorithm on JPEG spliced images has a better performance than other kinds of spliced images. At low Signal-to-Noise Ratio (SNR) of 30dB, the lowest 65.00% and the average 71.67% detection accuracy of the proposed algorithm are obtained.

Moreover, Fig. 6 compares the results of the scheme when the spliced images were compressed with JPEG

quality factors (Q) of 100, 90, 80, 70, 60 and 50. As can be observed, the proposed algorithm on noisy spliced images is more robust to JPEG compression than other kinds of spliced images. Even with low compression factor Q = 50, the lowest 70.00% and the average 74.67% detection accuracy of the proposed algorithm are still achieved.

## CONCLUSION

In this study, a novel detection technique based on SCBSS for spliced images was proposed. The given image is first performed characteristics domain transform. If the suspected image contained spliced region, in general, is unlikely to be completely consistent with characteristics in a sense in the rest of the image. So, the mixing matrix based on this characteristics domain can be estimated and then all source image blocks can be recovered. These image blocks allow identifying the spliced region and the background region. Experimental results show that the proposed technique has good segmentation for various splicing operation. The proposed method has good robustness against Gaussian noise and lossy JPEG compression.

## ACKNOWLEDGMENTS

This study was supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 12KJB510026, 12KJB510025), the National Natural Science Foundation of China (Grant No. U1204606) and the Scientific Research Foundation for the PhD (Nantong University, Grant No. 03080416, 03080415).

## REFERENCES

Chen, M., J. Fridrich, M. Goljan and J. Lukas, 2008. Determining image origin and integrity using sensor noise. IEEE Trans. Inform. Security Forensics, 3: 74-90.

Farid, H., 2009a. Exposing digital forgeries from JPEG ghosts. IEEE Trans. Inform. Forensics Sec., 4: 154-160.

Farid, H., 2009b. Image forgery detection. IEEE Signal Proces. Mag., 26: 16-25.

Hsu, Y.F. and S.F. Chang, 2010. Camera response functions for image forensics: An automatic algorithm for splicing detection. Trans. Inform. Forensics Security, 5: 816-825.

Johnson, M.K. and H. Farid, 2007. Exposing digital forgeries in complex lighting environments. IEEE Trans. Inform. Forensics Sec., 3: 450-461.

Liu, Q., X. Cao, C. Deng and X. Guo, 2011. Identifying image composites through shadow matte consistency. IEEE Trans. Inform. Forensics Sec., 3: 1111-1122.

Popescu, A.C. and H. Farid, 2005a. Exposing digital forgeries by detecting traces of resampling. IEEE Trans. Signal Process., 2: 758-767.

Popescu, A.C. and H. Farid, 2005b. Exposing digital forgeries in color filter array interpolated images. IEEE Trans. Signal Process., 53: 3948-3959.

Yao, H., S. Wang, Y. Zhao and X. Zhang, 2012. Detecting image forgery using perspective constraints. IEEE Signal Process. Lett., 3: 123-126.