Pixel-Based Image Forgery Detection: A Review

Yi-Hau Lai

Abstract

With the advancement of the digital image processing software and editing tools, a digital image can be easily manipulated. The detection of image manipulation is very important because an image can be used as legal evidence, in forensics investigations, and in many other fields. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image. This article aims to compare the accuracy of two detection methods for copying, moving, and stitching, as well as their robustness under interference such as noise and compression. The first detection method is to use svd algebra techniques to extract regional features and compare the similarity of features. The second method constructs a CNN model and uses the spatial rich model to initialize the weights of the first layer

**Keywords:** image forgery, CNN, svd, Splicing, Tampering

# INTRODUCTION

Forgeries are not new to mankind but are a very old problem. In the past it was limited to art and literature but did not affect the general public. Nowadays, due to the advancement of digital image processing software and editing tools, an image can be easily manipulated and modified [1]. It is very difficult for humans to identify visually whether the image is original or manipulated. There is rapid increase in digitally manipulated forgeries in mainstream media and on the Internet [2]. This trend indicates serious vulnerabilities and decreases the credibility of digital images. Therefore, developing techniques to verify the integrity and authenticity of the digital images is very important, especially considering that the images are presented as evidence in a court of law, as news items, as a part of medical records, or as financial documents. In this sense, image forgery detection is one of the primary goal of image forensics [3].

Digital image forgery detection techniques are classified into active and passive approaches. In the active approach, the digital image requires preprocessing of image such as watermark embedding or signature generation, which limits their application in practice [3].

Unlike the watermark and signature-based methods, the passive techniques do not need any digital signature to be generated or to embed any watermark.

Passive image forgery detection techniques roughly can be divided into five categories [4] as shown in Figure 1. Pixel-based techniques detect statistical anomalies introduced at the pixel level; format-based techniques leverage the statistical correlations introduced by a specific lossy compression scheme; camera-based techniques exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing; physical environment-based techniques explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and geometry-based techniques make measurements of objects in the world and their positions relative to the camera.

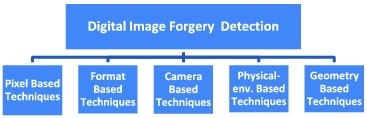


Figure 1: Digital image forgery detection techniques.

## Singular Value Decomposition

A novel framework for identifying the location of copy-move image tampering by applying the singular value decomposition (SVD). SVD served to produce algebraic and geometric invariant and feature vectors.

In SVD and reduced Rank approximation of a Matrix, the largest singular values (SVs) composes the k-dimension feature vector. SVs have some important properties of algebraic and geometric invariance and insensitiveness to noise. In recent years, singular values have been introduced as the feature vector for pattern recognition. Singular values features represent algebraic and geometric invariant properties of an image

## Deep Learning Approach

a novel image forgery detection approach that can automatically learn feature representations based on deep learning framework. The primary contributions are summarized as follows: (1) We first train a supervised CNN to learn the hierarchical features of tampering operations (splicing and copy-move) with labeled patches (p×p) from the training images. The first convolutional layer of the CNN serves as the pre-processing module to efficiently suppress the effect of image contents. Instead of the random strategy, the kernel weights of the first layer are initialized with the 30 basic high-pass filters used in calculation of residual maps in spatial rich model (SRM) [17], which helps to improve the generalization ability and accelerate the convergence of the network. (2) We then extract the features for an image with the pre-trained CNN on the basis of p×p patch by applying a patch-sized sliding-window to scan the whole image. The generated image representation is then condensed by a simple feature fusion technique, i.e. regional pooling, to obtain the final discriminative feature. (3) Finally, a SVM classifier is trained based on the resulting feature representation for binary classification (authentic/forged). The experimental results on several public datasets demonstrate that the proposed scheme can outperform some state-of-the-art methods.

# Singular Value Decomposition method

## General pixel-based process

## There are many approaches that have been proposed by various authors for detecting pixel-based image forgery. Figure 2 shows the general process of detecting copy-move image forgery.

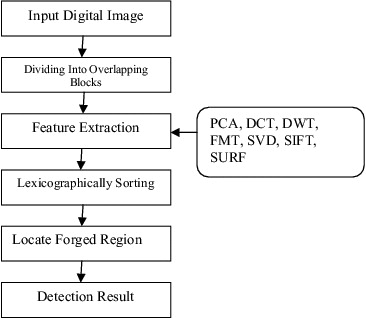


Figure 2: Block diagram of copy-move image forgery detection system

## SVD process

Singular Value Decomposition (SVD) is widely used in the field of pattern recognition, image and video compression, and signal processing. The image features extracted from SVD having algebraic invariant property. Hence, features are more stable compared to PCA. The steps involved in the detection of the copy-move

duplication regions using SVD algorithm are given as follows:

A forged *w* × *h* image is divided into fixed size overlapping *B* × *B* blocks.

SVD is applied to each block and their corresponding singular values matrices U, S, and V are extracted, expressed as

Where U and V are orthogonal matrices, and S is a diagonal singular value matrix of the form:

The diagonal elements of singular matrix, i.e., , , , . . . are the features of the block B that are stored in a row in the feature matrix.

The feature vectors of the blocks that are stored row-wise in a matrix called the feature matrix, arranged into lexicographical order.

The Euclidean distances D(u, v) between two rows, u and v, of the feature matrix, are calculated as

where u = (, , . . . , ) and v = (, , . . . , ).

All the block pairs, for which *D(p, q) > T*1 are eliminated. In the next step, further verification is executed on the remaining blocks.

The *Chebyshev distance* between two blocks u and v is calculated. Let u and v are the image blocks having coordinates (*i, j*) and (*k, l*), respectively. The Chebyshev distance is calculated as

If then blocks u and v are marked as duplicate blocks, where Ts is a user-defined value.

# Multimedia figures – video and audio files

Video and audio files can be included for publication. Table 3 lists the specifications for the mulitimedia files. Use a screenshot or another .jpg illustration for placement in the text. Use the file name to begin the caption. The text of the caption must end with the text "<http://dx.doi.org/doi.number.goes.here>" which tells the SPIE editor where to insert the hyperlink in the digital version of the manuscript.

Here is a sample illustration and caption for a multimedia file:



Video . A label of “Video/Audio 1, 2, …” should appear at the beginning of the caption to indicate to which multimedia file it is linked . Include this text at the end of the caption: <http://dx.doi.org/doi.number.goes.here>

Table 3. Information on video and audio files that can accompany a manuscript submission.

|  |  |  |
| --- | --- | --- |
| **Item** | **Video** | **Audio** |
| File name | Video1, video2, … | Audio1, audio2, … |
| Number of files | 0-10 | 0-10 |
| Size of each file | max. 5 mb | max. 5mb |
| File types accepted | .mpeg, .mov (Quicktime), .wmv (Windows Media Player) | .wav, .mp3 |

# Mathematical Equations

Use common fonts like Times Roman in your math equations. A math reference in a paragraph sentence such as  is not numbered. The steps of a mathematical argument can be numbered using a right-aligned tab for clarity, for example

α =  (1)

and

*ρ*=. (2)

# using THIS TEMPLATE AND ITS Automatic formatting

This document template and more information is available on SPIE.org:

<http://spie.org/x14101.xml> or by emailing [authorhelp@spie.org](mailto:authorhelp@spie.org)

## View the pre-formatted styles

To see the formats available with this manuscript, go to the Format menu and choose "Styles and Formatting". To view which style is being used in any part of this document, place your cursor on the line and look in the Styles and Formatting display.

## Using SPIE styles

To use this template in Microsoft Word: open this file and save it to a new file name. Type over the existing text with your paper. Alternately, you can delete all text, and select the SPIE style for each paragraph from the Styles and Formatting menu.

## Notes on SPIE styles

The styles listed in Table 2 automatically add extra spacing before and/or after paragraphs: SPIE title, SPIE authors-affiliations, SPIE section heading, SPIE subsection heading, and SPIE body text. The 1.1 Heading 2 style automatically goes into the body text style after one paragraph return.

References

1. Roy, A., Dixit, R., Naskar, R., Chakraborty, R. S., [Digital Image Forensics: Theory and Implementation], Springer,” (2020).
2. Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi., “Pixel-Based Image Forgery Detection: A Review,” IETE Journal of Education, 55:1, 40-46, (2014)
3. X. Kang and S. Wei, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics," 2008 International Conference on Computer Science and Software Engineering, 2008, pp. 926-930, (2008)
4. Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," 2016 IEEE International Workshop on Information Forensics and Security (WIFS), 2016, pp. 1-6, (2016)
5. Rathore, N.K., Jain, N.K., Shukla, P.K. et al. Image Forgery Detection Using Singular Value Decomposition with Some Attacks. Natl. Acad. Sci. Lett. 44, 331–338 (2021).