Blind Method for Image Forgery Detection: A tool for Digital Image Forensics

Anil Dada Warbhe
Asst. Professor, DEE, MIET, Gondia

R. V. Dharaskar
Director, MPGI Integrated Campus, Nanded

ABSTRACT
Undoubtedly, we are living in era of digital information and technology. In this revolutionized world of digital information, we are exposed to a remarkable array of visual imagery. With sophisticated image editing tools and software's, it is very easy to manipulate and temper the digital images, thereby questioning the trustworthiness of it. This paper presents a method based on a statistical technique, Independent Component Analysis (ICA), also known as a Blind Source Separation (BSS), to detect the copy-move kind of forgery in digital images. Results of this method prove that ICA can be effectively used for image forgery detection in digital image as a tool to digital image forensics.

General Terms
Digital Forensics, Image Processing.

Keywords
Digital forensics, Image processing, BSS, ICA, Image tempering.

1. INTRODUCTION
With the availability of low cost off the shelf image manipulation and cloning tools, it is very easy to tamper and create fake images even to a person with lukewarm skills of photography. Every now and then we are been presented with the amazing and sometimes unbelievable kind of images in our email inboxes. Maximum of it are nothing but artificially synchronized photographic fakes, adopted, for promoting and floating different stories through media, emails and social networking websites.

The manipulations done in the images cannot be detected and make out by naked eyes; as manipulations may not leave obvious evidence of tampering. The manipulation to change the original content of the image is also known as image fakery. Image fakery is a cybercrime, but because of the lack of proper regulatory framework and infrastructure for prosecution of such evolving cybercrime, leads to dissatisfaction about increasing use of such tools. This scene developed the feeling of cynicism and mistrust among civilians.

Over the past few years, the field of digital forensics has emerged to help restore some trust to digital images. Hence, to detect such modifications in the original content in the images needs to be detected, and hence, the necessity of algorithms for efficiently verifying the integrity of images cannot be overemphasized in this digital era.

2. RELATED WORK
Recently, numerous techniques for image integrity verifications have been proposed. Some techniques employ watermarking schemes [1] to authenticate an image as well as determine its integrity. The drawback with schemes based on watermarking is that the water mark must be embedded right during the image formation to avoid the possibility of watermarking an already forged image. This is practically difficult as most digital cameras and other image acquisition devices do not have instantaneous watermarking facilities.There are also various techniques that detect image tampering in absence of watermarks and signatures. Such techniques exploit the digital image underlining structures. For example, based on statistical correlation, Popescu et al [2] study resampling to detect image tampering. Gopi et al [3] use Artificial Neural Network and Auto Regressive coefficients to localize digital forgery. Such methods, however, are not robust to compression and other geometric processing.

Some researchers exploit camera 'fingerprints' to detect image tampering. For instance, Johnson et al [4] expose digital forgeries using Chromatic Aberration. The proposed method by Lukas and his colleagues [5] can detect image forgeries through exploiting Sensor Pattern Noise. Johnson et al [6] apply a variety of principles of Optical Physics such as lighting inconsistencies to establish the state of an image. Fridrich et al [7] use quantized Discrete Cosine Transform (DCT) coefficients to represent feature vectors in their proposed block matching based method of detecting cloning.

Each of the schemes mentioned above commands meaningful efficiency only in specific kinds of tampering.

The main aim of the image forgery detection especially that of a copy-move image forgery detection algorithm is to determine if a given image contains cloned regions without prior knowledge of their shape and location. An obvious approach is to exhaustively compare every possible pair of regions. However, such an approach is exponentially complex. Block matching appears to be a more efficient approach. Utilizing such an approach, A copy-move image forgery detection algorithm is proposed in [8], which slides a $b \times b$ block over an $N \times N$ image pixel by pixel resulting in $k = (N - b + 1)^2$ blocks. Each block is column-wisely reshaped into a b^2 long row vector, otherwise known as feature vector, and inserted into a $k \times b^2$ feature matrix. Principal Component Analysis (PCA) is performed to derive an alternative representation of each row of the feature matrix. PCA, which we present later in this section for the sake of completeness, is a well-known algebraic tool for matrix decomposition in literature [8]. Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) based method is proposed in [9], DWT is well explain in literature and widely used for its application to image processing[9], The proposed method in [10] uses the application of Principal Component Analysis-Eigenvalue Decomposition (PCA-EVD) in reducing the dimension of the feature vector while reducing the dimension of the image using DWT for the digital image forgery detection.

3. INDEPENDENT COMPONENT ANALYSIS

Recently, there has been an increasing interest in statistical models for learning data representations. A very popular method for this task is independent component analysis (ICA), the concept of which was initially proposed by Comon [11]. The ICA algorithm was initially proposed to solve the blind source separation (BSS) problem i.e. given only mixtures of a set of underlying sources, the task is to separate the mixed signals and retrieve the original sources [12]. Neither the mixing process nor the distribution of sources is known in the process. A simple mathematical representation of the ICA model is as follows.

Consider a simple linear model which consists of N sources of T samples i.e. $S_i = [S_i(1), ...,S_i(t),...,S_i(T)]$. The symbol there represents time, but it may represent some other parameter like space. M weighted mixtures of the sources are observed as X, where $X_i = [X_i(1),... ,X_i(t),... ,X_i(T)]$. This can be represented as –

$$X = A S + n; \quad (1)$$

Where
$X= (X_1, X_2, X_3……., X_M)$; $S= (S_1, S_2, S_3……., S_N)$ and $n= (n_1, n_2, n_3……., n_k)$.
S and n represent the additive white Gaussian noise (AWGN). It is assumed that there are at least as many observations as sources i.e. M = N. The M × N matrix A is represented as –

$$A=\begin{bmatrix} a_{11} & \cdots & a_{1} \\ \vdots & \ddots & \vdots \\ a_{M1} & \cdots & a_{N} \end{bmatrix}; \quad (2)$$

A relates *X* and *S*. *A* is called the mixing matrix. The estimation of the matrix *S* with knowledge of *X* is the linear source separation problem. The source separation problem cannot be solved if there is no knowledge of either *A* or *S*, apart from the observed mixed data *X*. If the mixing matrix *A* is known and the additive noise n is negligible, then the original sources can be estimated by evaluating the pseudo inverse of the matrix *A*, which is known as the un-mixing matrix *B*, such that

$$BX = BAS = S \quad (3)$$

For cases where the number of observations M equals the number of sources N (i.e. $M = N$), the mixing matrix A is a square matrix with full rank and $B = A^{-1}$.

The necessary and sufficient condition for the pseudo-inverse of *A* to exist is that it should be of full rank. When there are more observations than the sources (i.e. $M > N$), there exist many matrices *B* which satisfy the condition $BA = I$. Here the choice *B* depends on the components of S that we are interested in. When the number of observations is less than the number of sources (i.e. $M < N$), a solution does not exist, unless further assumptions are made. On the other side of the problem, if there is no prior knowledge of the mixing matrix *A*, then the estimation of both *A* and *S* is known as a blind source separation (BSS) problem. A very popular technique for solution of a BSS problem is independent component analysis [13]. Estimation of the underlying independent sources is the primary objective of the BSS problem. The problem defined in (3), under the assumption of negligible Gaussian noise n, is solvable with the following restrictions:

- The sources (i.e. the components of *S*) are statistically independent.
- At most, one of the sources is Gaussian distributed.
- The mixing matrix is of full rank.

From the above discussion, the following remarks can be made on ICA.

4. ALGORITHM

Basically almost all ICA algorithms are good for separation of the instantaneous mixture of the non-Gaussian sources. We here assume that the mixture is instantaneous. Firstly we feed two images,i.e., forged and original image, we mix both the images instantaneously.Then this mixture is fed to an improved version of the FastICA [13, 14]. We have used EFICA [15], algorithm which is asymptotically efficient, i.e., its accuracy given by the residual error variance attains the Cramér-Rao lower bound. The error is thus as small as possible. Finally, we get the estimated independent components as separate image output, making us able to identify the forged regions.

(a) (b)

Fig 1: The five head king cobra hoax, (a) a forged image (b)original image

Fig 2: extracted forged section and original image

(a) (b)

Fig 3: four student image, (a) a forged image (b)original image

Fig 4: extracted forged section from the forged image

5. CONCLUSION

In this paper we have presented a new approach to digital image forgery detection based on blind source separation using independent component analysis. The experiments included show how this new method successes in extracting and detecting the copy-move forgery if any in the image.

Though this method is good at detecting the forgery in the images the main limitation of this method is that, it needs the forged image as well as the original image which is been forged. This limitation can be overcome by using and applying a single channel independent component analysis on a single forged image to extract the forgery.

6. REFERENCES

[1] 1C. T. Hsieh and Y. K. Wu, "Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix," WSEAS Transaction on Signal Processing, Vol. 2, Issue 5, May 2006, pp.612-618.

[2] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling," IEEE Transactions on Signal Processing, Vol. 53, 2005, pp. 758-767.

[3] E. S. Gopi, N. Lakshmanan, T. Gokul, S. KumaraGanesh, and P. R. Shah, "DigitalImage Forgery Detection using Artificial Neural Network and Auto Regressive Coefficients," Electrical and Computer Engineering, 2006, pp.194-197.

[4] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration," in Proceedings of the 8th workshop on Multimedia and security, 2006, pp. 48-55.- 257

[5] J. Lukas, J. Fridich, and M. Goljan, "Detecting Digital Image Forgeries Using Sensor Patter Noise," in Proceedings of the SPIE Conference on Security Steganography, and Watermarking of Multimedia Contents, Vol. 6072, January 2006, pp. 362-372.

[6] M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting," in Proceedings of ACM Multimedia and Security Workshop, New York, 2005, pp.1-9.

[7] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," in Proceedings of Digital Forensic Research Workshop, August 2003

[8] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[9] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, July 2-5, 2007, pp. 1750-1753.

[10] Michael Zimba, Sun Xingming , "DWT-PCA (EVD) Based Copy-move Image Forgery Detection", International Journal of Digital Content Technology and its Applications. Volume 5, Number 1, January 2011

[11] P. Comon, "Independent Component Analysis-A new concept?" Signal Processing, vol. 36, pp. 287-314, 1994.

[12] J.F.Cardoso, "Blind Signal Separation: Statistical Principles", Proc. of IEEE, vol. 9, no. 10, pp. 2009-2025, 1998.

[13] AapoHyvärinen et al., "Independent Component Analysis: Algorithms and Applications", Neural Networks, 13(4-5):411-430, 2000.

[14] AapoHyvärinen et al., "Independent Component Analysis: Algorithms and Applications", Neural Networks, 13(4-5):411-430, 2000.

[15] A. Hyvarinen, "Fast and robust fixed-point algorithms for independent component analysis". IEEE Trans. Neural Netw.,vol.10,no.3,pp.624-634,May 1999.

[16] Koldovský, Z., Tichavský, P., and Oja, E.: Efficient Variant of Algorithm FastICA for Independent Component Analysis Attaining the Cram´er-Rao Lower Bound, IEEE Tr. Neural Networks, 17 (2006) 1265–1277.