ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 8, August 2014

Image Forgery Detection Techniques for Forensic Sciences

Mrs. Sharmila Sengupta[1]; Miss Prajakta Shinde[2]; Miss Hiral Shah[3]

[1]Assistant professor, V. E. S. Institute Of Technology; [2] B. E. Student, V. E. S. Institute Of Technology; [3] B. E. Student, V. E. S. Institute Of Technology;

sharmilase@yahoo.com; prajaktashinde.7@gmail.com; hiral.shah.06@gmail.com

ABSTRACT

Advancement in digitization has given rise to many image processing tools that help produce doctored Images with high sophistication, which are manipulated and yet the tampering is not easily visible to naked human eye. And with the user-friendliness offered by these image-processing tools, creating non-existing situations has become a very easy job and such manipulated digital images can be presented as evidence in a court of law. This diminishes the credibility of photographs as a definitive proof of events. The copy move forgery is one of the most common techniques of image tampering. In this paper we have discussed a copy move forgery detection system which uses duplicate region detection based on Singular Value Decomposition (SVD). Also for Splicing, which is another common technique of image tampering, we have proposed a detection system which is based on Canny edge detection. Also, face recognition is a very valuable aspect of criminal investigation, thus, we have also discussed face recognition using PCA algorithm. Adding on, we have also discussed Double Quantization Effect in JPEG images and its detection, which implies that the JPEG image was re-saved after it was opened with a photo editor.

General Terms

Image Processing, digital images, SVD, PCA.

Keywords

Forgery Detection, Copy-Move Forgery, Double Quantization Effect, Splicing, SVD, PCA, Face recognition.

1. INTRODUCTION

In this age of digitization we are always surrounded by digital images, in newspapers, in courtrooms, and all over the Internet. We are exposed to them for most of the time of the day. Ease with which images can be manipulated; we constantly need to be aware of the fact that seeing does not always imply believing. Over the past few years, the world has witnessed tremendous growth in the use of digital photography, a trend which opens the door for new and creative ways for forging images. Now a day's plenty of software's are available, sometimes even free of cost, that are used to manipulate image and even after doing so, the image looks like the original one itself. Thus, detecting such types of forgeries has become a serious issue at present. To find the marks of tampering in a digital image is a big challenge.

For digital photographs to be used as evidence in legal matters or to be distributed in mass media, it is absolutely necessary to identify whether an image is authentic or not. For the news photographs and the electronic check clearing systems, image authenticity becomes extremely critical. The verification of originality of images is required in many other variety of fields such as military, forensic, media, scientific, glamour, etc. Digital Image Forensics is concerned with the problem of certifying the authenticity of a picture, without any explicit a priori information, e.g. using watermarks. There exist three main categories in this field of research: image source identification; discrimination of computer generated images; image forgery detection. In this paper we have focused on the problem of detecting some of the image forgeries.

Images have always played an important part in forensic studies and law enforcement; for instance, images of criminals, images of crime scenes, biometric images, etc. When these images are produced as evidences in courtrooms, verifying integrity of images is of great importance. Images are used as authenticated proof for any crime and if integrity of those images itself is in question, then it will create a problem. Most of the applications that use digital images are sensitive applications; like a judgment made in a courtroom based on an image produced as evidence, etc. Thus it becomes very important to design and deploy efficient and effective approaches to detect image forgeries.

2. FORGERY ANALYSIS IN FORENSIC

2.1 Questioned Documents:

Crime scene investigation, DNA testing, fiber analysis, fingerprint analysis, voice identification and narcotics analysis, handwriting analysis.

2.2 Art Forgery:

It is the creating and selling of works of art which are falsely credited to other, usually more famous, artists.

2.3 Image Forgery [1], [2], [10]:

2.3.1 Copy-Move Forgery:

Images tampered by copying one area in an image and pasting it onto another area. It is called as Copy-Move Forgery or Cloning. This forgery is copying and pasting areas from one or more images and pasting on to an image being forged.

2.3.2 JPEG Format Analysis:

The JPEG Format Analysis algorithm makes use of information stored in the many technical meta-tags available in the beginning of each JPEG file. These tags contain information about quantization matrixes, Huffman code tables, and many other parameters as well as a miniature version (thumbnail) of the full image.

2.3.3 Double Quantization Effect:

Based on certain quantization artifacts appearing when applying JPEG compression more than once. If a JPEG file was opened, edited, then saved, certain compression artifacts will inevitably appear.

2.3.4 Error Level Analysis:

It detects foreign objects injected into the original image by analyzing quantization tables of blocks of pixels across the image.

2.3.5 Nonconsistent Image Quality:

JPEG is a lossy format. Every time the same image is opened and saved in the JPEG format, some apparent visual quality is lost and some artifacts appear.

2.3.6 Mixed Images:

Images generated by Splicing (combining two images), Scaling and Tilting (copying a object and applying geometrical transform on it).

3. COPY MOVE FORGERY

Copy-Move is one of the most commonly used techniques and is a specific type of image manipulation, where a part of the image itself is copied and pasted into another part of the same image.

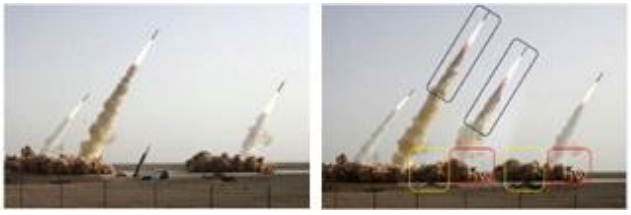

Figure 1. An example of copy-move forgery: (a) the original image with three missiles (b) The forged image with four missiles.

Copy-Move forgery is performed with the intention of either making an object "invisible" from the image by covering it with a small block of background, copied from another part of the same image or create additional copy of an object already existing in the image by copying it to the desired location. Since the copied segments are part of the same image, the color palette, noise components, dynamic range and the other properties will be consistent with the rest of the image, and thus making it is very difficult for a naked human eye to detect the forgery. Sometimes, even it is harder for technology to detect the forgery, if the image is retouched.

There are many Copy-Move Forgery detection techniques available. However, in most other approaches the forged image is follow following algorithm[3]:

1. Let N be the total number of pixels in a grayscale or color image.
2. Initialize the parameters:
   - b: number of pixels per block ($\sqrt{b}$ × pixels in dimension) - there are $N_b = (\sqrt{N} - \sqrt{b} + 1$ such blocks.
   - Nn: number of neighboring rows to search in the lexicographically sorted matrix
   - Nf : minimum frequency threshold
   - Nd: minimum offset threshold
3. Dividing the into overlapping blocks of size b.
4. Feature Extraction**:** Using SVD, compute singular values using $A=USV^T$ where U=AA*, V=A*A and S is the non-zero singular values of A are the square roots of the non-zero eigenvalues of both A*A and AA*. Different feature extraction methods can be used like PCA, DCT, DWT, [3], [4] etc.
5. Build a N_b × matrix whose rows are given by the singular values.
6. Sort the rows of the above matrix in lexicographic order to yield a matrix S. Let S_i denote the rows of S, and let (x_i, y_i) denote the position of the block's image coordinates (top-left corner) that corresponds to S_i.
7. Locate similar blocks**:**
   - For every pair of rows S_i and S_j from S such that $|i - j| < Nn$, place the pair of coordinates$(\mathbf{x_i}, \mathbf{y_i})$ and $(\mathbf{x_j}, \mathbf{y_j})$ onto a list.
   - For all elements in this list, compute their offsets, defined as:
     $(x_i - x_j , y_i - y_j)$ if $x_i - x_j > 0$
     $(x_j - x_i , y_i - y_j)$ if $x_i - x_j < 0$
     $(0 , |y_i - y_j|)$ if $x_i = xj$
   - Discard all pairs of coordinates with an offset frequency less than Nf .
   - Discard all pairs whose offset magnitude, $\sqrt{(\mathbf{x}_i - \mathbf{x}_j)^2 + (\mathbf{y}_i - \mathbf{y}_j}$, is less than Nd.
   - From the remaining pairs of blocks build a duplication map by constructing a zero image of the same size as the original, and coloring all pixels in a duplicated region with a unique gray scale intensity value.

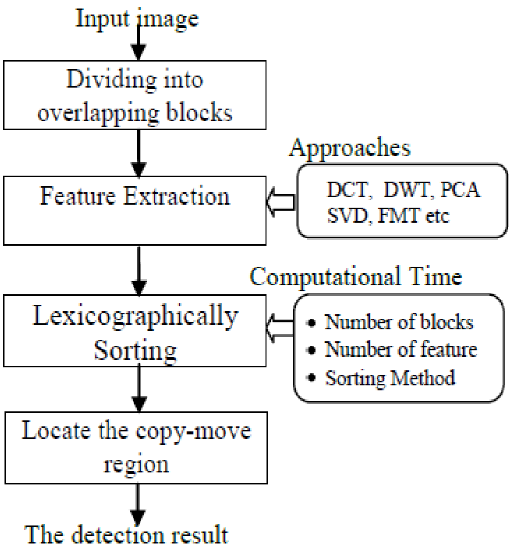

Figure 2. Configuration of a block Copy-Move Digital Image Forgery Detection System [4]

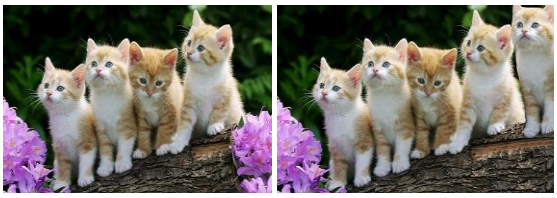

Figure 3. (a)The original image (b) Forged image

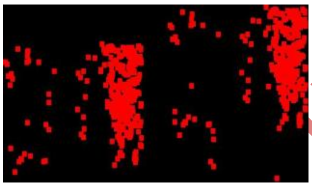

Figure 3. (c) Output of copy-move forgery detection by SVD.

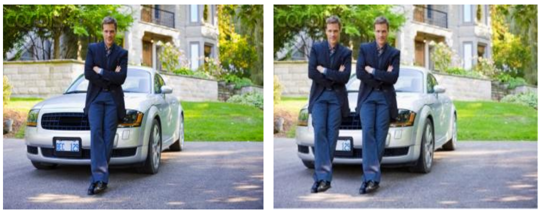

Figure 4. (a)The original image (b) Forged image

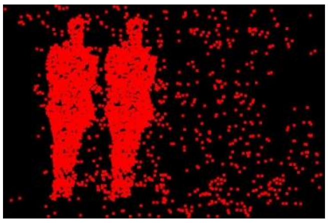

Figure 4. (c) Output of copy-move forgery detection by SVD.

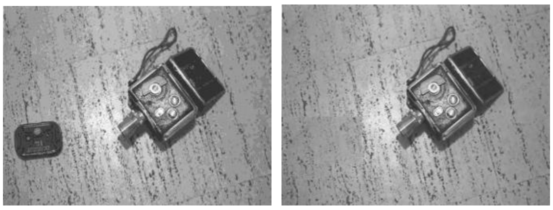

Figure 5. (a)The original image (b) Forged image

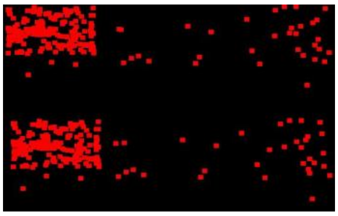

Figure5. (c) Output of copy-move forgery detection by SVD.

4. SPLICING

It is a method of manipulating images by combining two different source images to produce a new image which retains the majority of one image for detail. Figure 6 is an example of a spliced image.

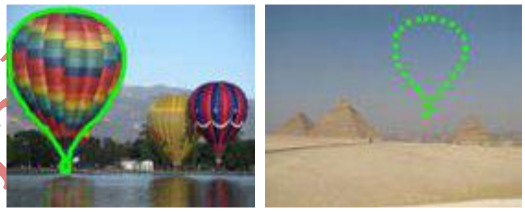

Figure 6. (a) Source image (b) Target image

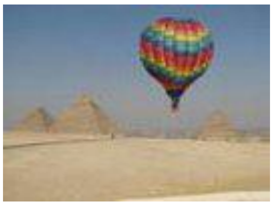

Figure 6. (c) Spliced image

Splicing is basically copying areas from one or more images and pasting them on to an image being forged. The image processing community formally refers to this type of image as an image "composition," which is defined as the "digitally manipulated combination of at least two source images to produce an integrated result".

Most of the Splicing forgery detection techniques are based on JPEG compression threshold, which limits their suitability to only JPEG image format. But today there exist such advanced digital cameras, that support other image formats as well. For this reason, novel methodology for photo forgery detection based on standard deviation based edge detection that detects the edges present in all directions was devised.

The following steps explain the process of splicing forgery detection [5]:

1. *Image Pre-processing:*

If the image data is not represented in HSV color space, it is converted to this color space by means of appropriate transformations. We only use the intensity data (v-channel of HSV) during further processing. Here V Channel represents the intensity image.

2. *Edge Detection:*

This step focuses the attention to areas where tampering may occur. We employ a simple method for converting the gray-level image into an edge image. Using Canny Edge detection us extract the edge image. Many other edge detection techniques can be used.

3. *Detection of Forged Region:*

The forged region is the one where there appears an edge even if it's not visible in the acquired photo.

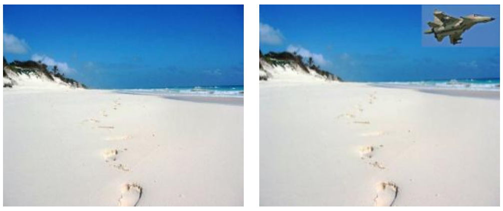

Figure 7. (a) The original image (b) Forged image

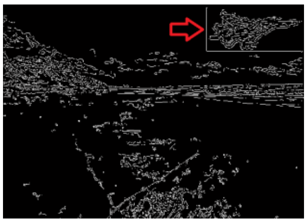

Figure 7. (c) Output of splicing detection by Canny edge detector.

5. DOUBLE QUANTIZATION EFFECT

While modifying JPEG image, usually it is loaded into a photo–editing software (decompressed) like, Adobe Photoshop and after manipulations are carried out, the image is re–saved (compressed again). The quantization matrix of the original image is called as primary quantization matrix. And the quantization matrix of the re–saved image is called as secondary quantization matrix. If the primary and secondary quantization matrix are not identical, then the act of re–saving (double compression) brings into the image specific changes.

Certain quantization artifacts appear when applying JPEG compression more than once. If a JPEG file was opened, edited, then saved, certain compression artifacts will inevitably appear [1].

Figure 8. (a) & (b) These two images look identical, although the second picture was opened in a graphic editor and then saved again.

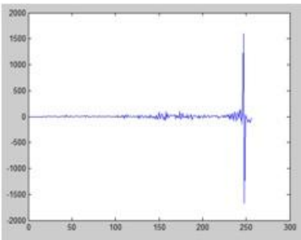

Figure 8. (c) Difference in the histograms of images shown above.

6. RECOGNITION

PCA (Principal Component Analysis) is one of the most significant techniques in image recognition and feature extraction. Here we are using PCA for recognizing stamps and detecting whether stamp is forged one or not and as well as for face recognition of criminals and any other object.

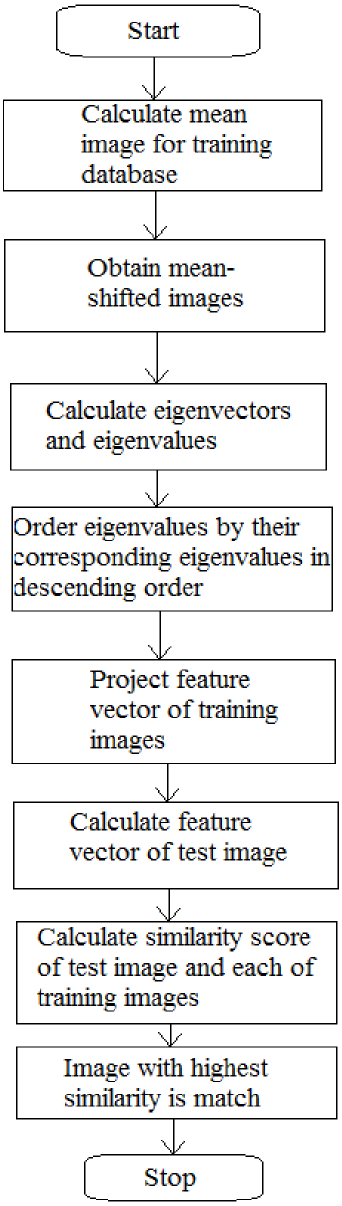
Start
Calculate mean image for training database
Obtain mean-shifted images
Calculate eigenvectors and eigenvalues
Order eigenvalues by their corresponding eigenvalues in descending order
Project feature vector of training images
Calculate feature vector of test image
Calculate similarity score of test image and each of training images
Image with highest similarity is match
Stop

Figure 9. Recognition using PCA.

PCA of a matrix is given by [6]:

- Denote column vectors xi ∈ Rn, i = 1, ..., N as the input data.
- The overall mean is: $\mu = \frac{1}{N}\sum_{i=1}^{N}$
- The zero-meaned data is packed into a n×N matrix:
  $M = (x_1 - \mu \ x2 - \mu \ ..... xN - \mu)$
- The n x n covariance matrix is computed as :
  $C = MM^T$
- The principle components are the eigenvectors ej of the covariance matrix (i.e., Cjej=λjej),where the eigenvalue, λj is proportional to the variance of the original data along the j^{th} eigenvector.)

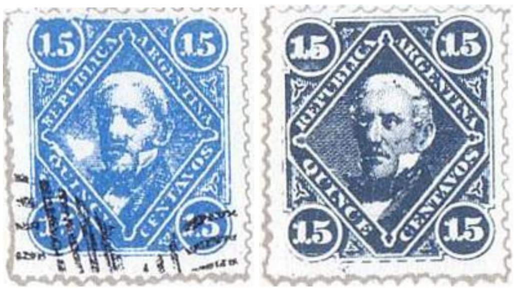

Figure 10. (a)Forged stamp, (b) Original stamp. Comparing these two images after recognizing the original stamp we get to know the stamp is forged.

Figure 11. (a) Image acquired, (b) Output image given by the recognition software. The software recognizing the person properly can be used for recognizing criminals in forensics.

Figure 12. (a) Image acquired, (b) Output image recognized by the software. This software can also be used to recognize other object like flowers, animals, etc.

Different version of PCA can be used to increase the speed and accuracy of the software [7], [8], [9].

7. CONCLUSION

Most of the confidential forgery detection requires an Optical Laboratory which uses magnifiers, high-powered microscopes (micro and macro objectives), polarizer, complete spectral analyzers, including infrared, ultraviolet (short and long wave) and LASER fluorescence amplification technologies. Using MATLAB, we have reviewed and implemented few algorithms for detection of some of the common types of forgeries. There is a lot of research going on in this field and many other tampering detection techniques have been devised such as, detection based on examining the lighting environment, camera feature based detections, studying the statistical and geometric properties etc. Moreover, advancement in image forgeries necessitates detection techniques that make use of artificial intelligent, expert system, common sense reasoning, and machine learning technologies from the perspective of simulating human thought.

8. REFERENCES

[1] Alexey Kuznetsov, Yakov Severyukhin, Oleg Afonin, Yuri Gubanov, “Detecting Forged (Altered) Images”, Forensics Focus - Articles.

[2] G. R. Elwin J , Aditya T S , M. Shankar S,” Survey on Passive Methods of Image Tampering Detection”, International Conference on Communication and Computational Intelligence, 2010,pp .431-436.

[3] Frank Y. Shih,Yuan Yuan, “A Comparison Study on Copy-Cover Image Forgery Detection”, The Open Artificial Intelligence Journal, 2010,pp. 49-54.

[4] B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo, “Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods”, Global Journal of Computer Science and Technology, 2010, Vol. 10, Issue 7, pp. 61-65.

[5] S.Murali, G. B. Chittapur, Prabhakara H. S, B. S. Anami, “Comparison and Analysis of Photo Image Forgery Detection Techniques”, International Journal on Computational Sciences & Applications (IJCSA), 2012, pp.45-56

[6] Hany Farid, “Dgital Image Forensics”, pp. 68-69.

[7] Sergiu Nedevschi, “An improved PCA type algorithm applied in face recognition”, International Conference on Intelligent Computer Communication and Processing (ICCP), 2010, pp. 259-265.

[8] Nedevschi S, Peter I.R., Dobos I.A., Prodan C., ”An improved PCA type algorithm applied in face recognition”, IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2010, pp. 259-265.

[9] Bozorgtabar B., Noorian, F., Rezai Rad G.A., “Comparison of Different PCA based face recognition algorithms using genetic programming”, 5th International Symposium on Telecommunications (IST), 2010,pp. 801-805.

[10] Pradyumna Deshpande , Prashasti Kanikar, “Pixel Based Digital Image Forgery Detection Techniques”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 539-54.