ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

A Review of Image Forgery Techniques

Hardish Kaur, Geetanjali Babbar

Assistant professor, CGC Landran, India.

ABSTRACT: Image forgery refer to copying and pasting contents from one image into another image. This procedure is quite common now these days. This process is done to earn money in a wrong way and to hide the originality of the image. This paper focuses on the methods of detection of the image forgery and the aspects of the image forgery . This paper also focuses on the classification methods of the image forgery**.**

KEYWORDS: IMAGE FORGERY , IMAGE PROCESSING , CLASSIFICATION

I. INTRODUCTION

The trustworthiness of photographs has an essential role in many areas, including: forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. The art of making image fakery has a long history. But, in today's digital age, it is possible to very easily change the information represented by an image without leaving any obvious traces of tampering. Despite this, no system yet exists which accomplishes effectively and accurately the image tampering detection task.The digital information revolution and issues concerned with multimedia security have also generated several approaches to digital forensics and tampering detection. Generally, these approaches could be divided into active and passive–blind approaches. The area of active methods simply can be divided into the data hiding approach (e.g., watermarks) and the digital signature approach. We focus on blind methods, as they are regarded as a new direction and in contrast to active methods, they work in absence of any protecting techniques and without using any prior information about the image. To detect the traces of tampering, blind methods use the image function and the fact that forgeries can bring into the image specific detectable changes (e.g., statistical changes).When digital watermarks or signatures are not available, the blind approach is the only way how to make the decision about the trustworthiness of the investigated image. Image forensics is a burgeoning research field and promise a significant improvement in forgery detection in the never–ending competition between image forgery creators and image forgery detectors.The example in Figure shows two digital images. The left image was printed by several news sources in an article about a mysterious giant-sized "hogzilla" [19]. While the authenticity of the image is unknown, with very little skill a "forged" version was digitally created using the computer software Adobe Photoshop. It is very hard, if impossible, for the human eye to detect digital manipulation at face value. This is just one example of the need for a tool to aid in the detection of digital image tampering. The research in this thesis attempts to address this need and provide some insight into this challenging problem

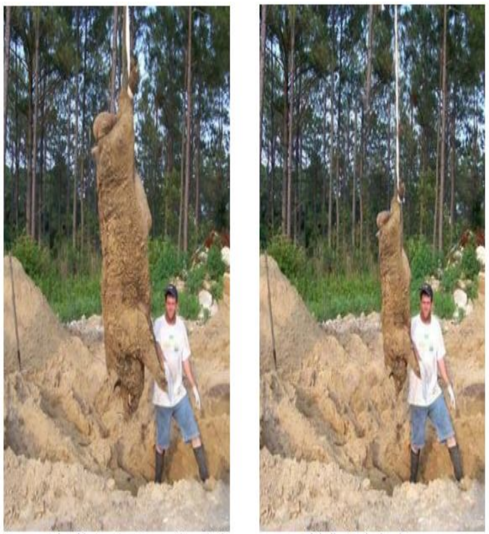


Image as Printed in San Jose Mercury News [19]

Digitally Manipulated Image

Local Binary Pattern. LBP is a kind of gray-scale imageure operator which is usedfor describing the spatial structure of the image imageure . The imageure T in a localneighborhood of a gray scale image can be defined as the joint distribution of the graylevels of P(P > 1) image pixels using the following equation
where p is the total number of pixels in asset and t is the local binary pattern I the same image .

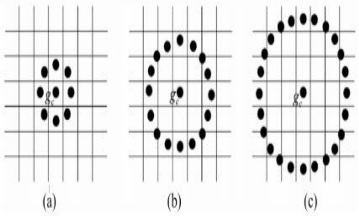


FIGURE 1. Circular symmetric neighbor sets for different (P, R) [9]. (a) (P, R)=(8,1), (b) (P,R)=(16,2), (c) (P,R)=(24,3).

$$T= gc(t0,t1\ldots\ldots\ tp-1)$$

With techniques available to protect an original image from tampering, the reverse scenario raises concern of verifying the authenticity of an image of unknown origin. This is an increasingly important issue as digital cameras come down in price and ease of use of powerful image processing software, i.e. Adobe Photoshop and GIMP (GNU Image Manipulation Program), become more widely available [15]. In fact, GIMP is freely available on the web and is a viable alternative to Adobe Photoshop. Most of the image manipulations discussed in this thesis can be performed using GIMP. With increasing opportunities and ease to digitally manipulate images, the research community has its work cut out.The state of the art in research in digital image forensics currently focuses on digital watermarking and variations of this, as previously discussed. Research conducted on image authentication in the absence of any digital watermarking scheme is still in its infancy stages [9] [12].

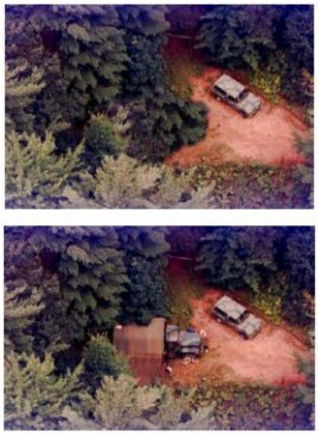


Figure 2.3 – Example of *copy-move* image forgery [12]

II. CLASSIFIERS IN THE PROCESS OF IMAGE TEMPERING

A. Support Vector Machine (SVM)

Support vector machine classifier is used to make segments of selected data on the basis of emotions and simple image. Input data is presented in two sets of vectors in n-dimensional space, a separate hyper-plane is constructed in space due to which margin between two data sets maximize.

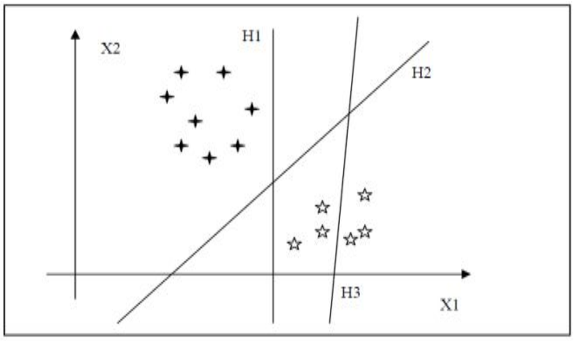
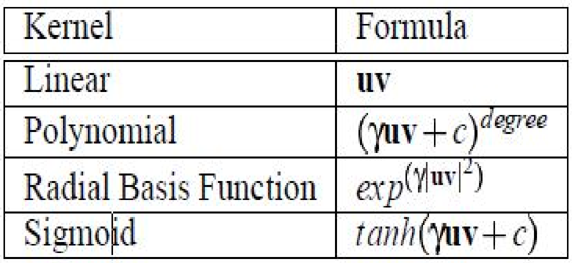


Figure represent s the SVM classifier

Kernel Function: During training a user need to define four standard kernels as following. A kernel function use of parameters such as γ, *c*, and *degree* that defined by user during training.



Kernel	Formula
Linear	$\mathbf{uv}$
Polynomial	$(\gamma\mathbf{uv}+c)^{degree}$
Radial Basis Function	$exp^{(\gamma\lvert\mathbf{uv}\rvert^{2})}$
Sigmoid	$tanh(\gamma\mathbf{uv}+c)$

A. NAÏVE BAYES CLASSIFIER

Naïve Bayes is used as image classifier because of its simplicity and effectiveness. Simple(“naive”)classifica1onmethodbased on Bayesrule [7]. The Bayes rule is applied on document for the classification of image. The rule which is following is:

$$P(c\,|\,d) = \frac{P(d\,|\,c)P(c)}{P(d)}$$

This rule is applied for a document d and a class c. probability of A happening given to B can be find with the probability of B given to A. this algorithm work on the basis of likelihood in which probability of document B is same as frequency of words in A.on the basis of words collection and frequencies a category is represented. We can define frequency of word is number of time repetition in document define frequency of that word. We can assume n number of categories from C_0 to C_{n-1}. Determining which category a document D is most associated with means calculating the probability that document D is in category C_i, written $P(C_i|D)$, for each category C_i.

Using the Bayes Rule, you can calculate $P(C_i|D)$ by computing:

$P(C_i|D) = (P(D|C_i) * P(C_i)) / P(D)$

$P(C_i|D)$ is the probability that document D is in category C_i; in document D bag of words is given by probability, which create in category C_i. $P(D|C_i)$ is the probability that for a given category C_i, the words in D appear in that category.

$P(C_i)$ is the probability of a given category; that is, the probability of a document being in category C_i without considering its contents. P(D) is the probability of that specific document occurring. We can classify image with procedure that required using above discussed parameters is as following:

III. BACK PROPAGTION NEURAL NETWORK

A bpa neural network (BPANN) is a feed-forward, artificial neural network that has more than one layer of hidden units [7] between its inputs and its outputs. Each hidden unit, j, typically uses the logistic function1 to map its total input from the layer below, xj , to the scalar state, yj that it sends to the layer above.

y_j= logistic(xj) =1/1 + e^{-xj}, x_j = bj +$\sum y_i$ w $_{ij}$

where bj is the bias of unit j, i is an index over units in the layer below, and wij is a the weight on a connection to unit j from unit i in the layer below. For multiclass classification, output unit j converts its total input, xj , into a class probability, pj.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

IV. CONCLUSION

The above paper classifies the ways of image tempering and classification methods and the ways of classification using different classifiers . The paper also describes a comparative study of the Support Vector Machines , Naïve Bayes Classification and the Neural Network Classification methods . The future research workers may use one of the above classification methods or a combination of the above classification methods .

REFERENCES

1. "JPEG2000," *TheFreeDicitionarydotcom*. August 18, 2004.http://encyclopedia.thefreedictionary.com/JPEG%202000.
2. "Myths & Facts about JPEG," *Graphics Software at About.com*. August 18, 2004.http://graphicssoft.about.com/library/weekly/aa0104jpegmyths.htm.
3. "What is Wavelet Analysis?" *Wavelet Toolbox Documentation*. MATLABversion 6.5. The MathWorks, Inc. 2002.
4. Associated Press, "Britain Says Soldier Held in Photo Probe." *Newsday* May 18, 2004. http://www.newsday.com/news/nationworld/world/wire/sns-ap-britainprisoner-abuse,0,4827144.story?coll=sns-ap-world-headlines.
5. Baxes, G. A., *Digital Image Processing : Principles and Applications*. New York: John Wiley & Sons, Inc, 1994.
6. Brinkmann, R., *The Art and Science of Digital Compositing*. San Diego:Academic Press, 1999.
7. Chandramouli, R., N. Memon, and M. Rabbani, *Encyclopedia of Imaging Scienceand Technology: Digital Watermarking*. J. Hornak, Editor. John Wiley, October2001.
8. Fan, Z. and R. L. de Queiroz, "Identification of Bitmap Compression History:JPEG Detection and Quantizer Estimation," *IEEE Transactions on ImageProcessing*, Vol. 12, No. 2: 230-235, February 2003.
9. Farid, H. and A. Popescu, "Exposing Digital Forgeries by Detecting Traces of Resampling."*Proceedings of the IEEE Transactions on Signal Processing*. (In Press). 2004.
10. Fridrich, J., R. Du, and M. Goljan, "Steganalysis Based on JPEG Compatibility,"Special session on Theortical and Practical Issues in Digital Watermarking and Data Hiding, *Multimedia Systems and Applications IV*. Pp. 275-280. Denver, CO,August 2001.
11. Fridrich, J. and J. Lukas, "Estimation of Primary Quantization Matrix in DoubleCompressed JPEG Images." *Proceedings of DFRWS 2003*. Cleveland, OH,August 2003.
12. Fridrich, J., J. Lukas, and D. Soukal, "Detection of Copy-Move Forgery in DigitalImages." *Proceedings of DFRWS 2003*. Cleveland, OH, August 2003.\
13. Guggenheim, K. "New Prison Abuse Photos Outrage Lawmakers." *Phillyburbs*May 13, 2004. http://www.phillyburbs.com/pb-dyn/news/27-05132004-299158.html.
14. Johnson, R. C. "JPEG2000 Wavelet Compression Spec Approved," August 18,2004. http://www.us.design-reuse.com/news/news1917.html.
15. Katzenbeisser, S. and F. Petitcolas, A.P. *Information Hiding – techniques forsteganography and digital watermarking*. Boston: Artech House, 2000.
16. Klasen, L. *Image Sequence Analysis of Complex Objects*. PhD dissertation.Linkoping University, Sweden, 2002.
17. Lukas, J. "Digital Image Authentication Using Image Filtering Techniques."*Proceedings of 15th Conference of Scientific computing "Algoritmy 2000"*,Vysoke Tatry-Podbanske, Slovakia, September 2000.
18. Luong C. M. "Introduction to Computer Vision and Image Processing," Department of Pattern Recognition and Knowledge Engineering, Institute ofInformation Technology, Hanoi, Vietnam, May 4, 2004.http://www.netnam.vn/unescocourse/computervision/computer.htm.
19. Minor, E. (Associated Press) "Hogzilla! Huge pig has small town talking, but is ita hoax?" *San Jose Mercury News*, July 29, 2004. sec. 3A.
20. Sachs, J. *Digital Image Basics*. Digital Light & Color. 1999.
21. Saha, S. "Image Compression – from DCT to Wavelets: A Review," May 28,2004 http://www.acm.org/crossroads/xrds6-3/sahaimgcoding.html.