ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Image Forgery Detection Using Svm Classifier

Anita Sahani[1], K.Srilatha[2]

M.E. Student [Embedded System], Dept. Of E.C.E., Sathyabama University, Chennai, India [1]

Assistant Professor, Dept. Of E.C.E, Sathyabama University, Chennai, India [2]

Abstract: In this paper, a method is developed for detecting image forgery including removal, insertion, and replacement of objects. SVM classifier is used which have similar functional form to neural networks. Image, texture and pixel value based features are extracted and analyzed from the images. Then hash values are calculated for these features. The process consists of two phases which are training phase and a testing phase. SVM classifier is trained with a set of images. SVM classifiers are used to classify the images as genuine or forged. For the secure use, RSA algorithm can be applied so that only authorized person can run the application to check whether the given query image is genuine or forged.

Keywords: Image forgery, SVM classifier, manipulation, hash values, RSA key.

I. INTRODUCTION

We are living in an age, where anything can be manipulated or altered with the help of modern technology. Today's digital technology had begun to erode the integrity of images. With the increasing applications of digital imaging, different types of software tools are introduced for image processing. They are used to combine two images to make it look real or objects can be added or deleted. Image forgery detection is generally classified as active and passive. The former detects the integrity of images by checking the change in digital watermark embedded either at the instant of image acquisition or before image distribution. The latter exploits only the knowledge of images themselves for forgery detection. Forgery is a subjective word. An image can become a forgery based on the context in which it is used. The manipulation techniques include deletion of details, insertion of details, combining multiple images and false captioning. Detecting these image manipulations has become an important problem. The types of forgery which can be identified are image that is created using software tools, created by altering its content or context. In other words in digital image forgery we change the material elements of an image and represent the changes as true copies of a real one.

II. RELATED WORK

Images have been a powerful media of delivering and communicating information. People have been doing manipulations with images in almost every field like fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, etc. Now it's a digital age where everything is possible. Many methods have been developed to detect image forgery. In this paper [1], a detailed evaluation of multi-scale Weber local descriptors (WLD) based image forgery detection method is presented. Multiscale WLD extracts the features from chrominance components of an image, which usually encode the tampering information that escapes the human eyes. This paper [2] presents a method to detect the forged images of people using the illuminant color. A forgery detection method is proposed by using pixel illumination level algorithm is used for the detection purpose. Duplication is identified by matching each pixel in the image. A Histogram of Oriented Gradient algorithm (HOG) is used for color illumination difference. A SVM classifier can be learned from training data of relevance images and irrelevance images marked by users. Various image hashing methods have been proposed. That has become a routine practice in many image hashing methods. Many previous schemes are either based on global or local features. In this paper [3], an image hashing method is developed using both global and local features. The global features are based on Zernike moments representing the luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image. This paper [4] presents methods for authenticating and identifying forged regions in images that have been acquired using flatbed scanners. The methods are based on using statistical features of imaging sensor pattern noise as a fingerprint for the scanner. An anisotropic local polynomial

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

estimator is used for obtaining the noise patterns. A SVM classifier is trained for using statistical features of pattern noise for classifying smaller blocks of an image.

III. PROPOSED METHOD

In the proposed method, SVM classifier is employed for forgery detection after calculating the hash values for extracted features.RSA key is set in training phase and the user is asked to enter the same key in testing phase to ensure that the user is an authorized person. SVM can model complex, real-world problems such as text and image classification, hand-writing recognition, and bioinformatics and bio-sequence analysis. We design a simple process consisting of two phases which are training phase and testing phase. The module description is as follows:

A. Database

A database is created and trained in the training phase with a number of images. The jpg and jpeg images can be either downloaded from the Internet or captured using digital cameras. The images can be of different sizes.

B. RSA key

The RSA key is set after training images in the database. When any user tries to run the application for checking the authenticity of query image, he has to enter the same key which was set during the training phase. Thus making sure that only authorized person can run the application.

C. Pre-processing

The images are converted into gray scale from rgb .Median filter is applied to remove noises present in the images. Image enhancement techniques are applied. It includes gray level & contrast manipulation, noise reduction, edge crispening and sharpening, filtering, interpolation and magnification, pseudo colouring, and so on.

D. Feature extraction

The features shown in fig.1 below are extracted from the images.

1) Image analysis: In the image analysis, the edges are analysed using the sobel or canny operator in the MATLAB.

2) *Pixel value analysis:* The mean and standard deviation are calculated for the images. . Mean Gray Value - Average gray value within the selection. This is the sum of the gray values of all the pixels in the selection divided by the number of pixels. Standard Deviation - Standard deviation of the gray values used to generate the mean gray value.

3) *Texture analysis:* Texture analysis can be used to find the texture boundaries. Texture analysis refers to the characterization of regions in an image by their texture content. The GLCM functions characterize the texture of an image by calculating how often pairs of pixel with specific values and in a specified spatial relationship occur in an image, creating a GLCM, and then extracting statistical measures from this matrix For texture analysis haralick function is used and the gray co-matrix function. The gray- level co-occurrence matrix (glcm) includes calculating energy, correlation, variation and entropy parameters.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

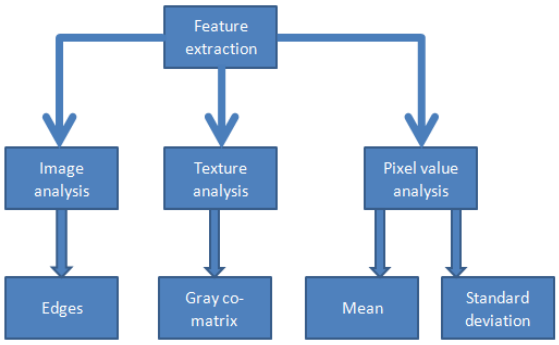

Fig.1: Feature extraction

E. Hash values

The hash values are calculated for the above extracted features.

F. SVM classifier

SVM determine the decision boundaries in the training step and the method can also provide good generalization in high dimensional input spaces. SVM classification is based on the concept of decision planes that define decision boundaries. A decision plane is one that separates between a set of objects having different class memberships. SVM finds the vectors ("support vectors") that define the separators giving the widest separation of classes. SVM classification supports both binary and multiclass targets. SVM models have similar functional form to neural networks and radial basis functions, both popular data mining techniques. However, neither of these algorithms has the well-founded theoretical approach to regularization that forms the basis of SVM. The quality of generalization and ease of training of SVM is far beyond the capacities of these more traditional methods. The SVMs map the original data points from the input space to a high dimensional, or even infinite-dimensional, feature space making classification problem simpler in feature space. The mapping is done by a suitable choice of a kernel function.

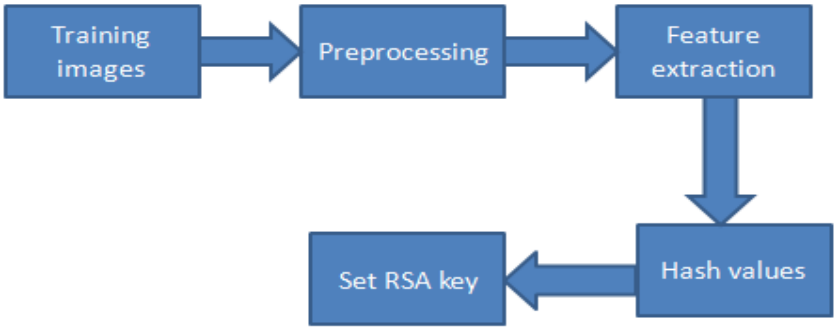

Fig.2: Training Phase

The training phase is shown in fig.2, where the images are trained, preprocessed and feature extraction is done. Then hash values are calculated and RSA key is set.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

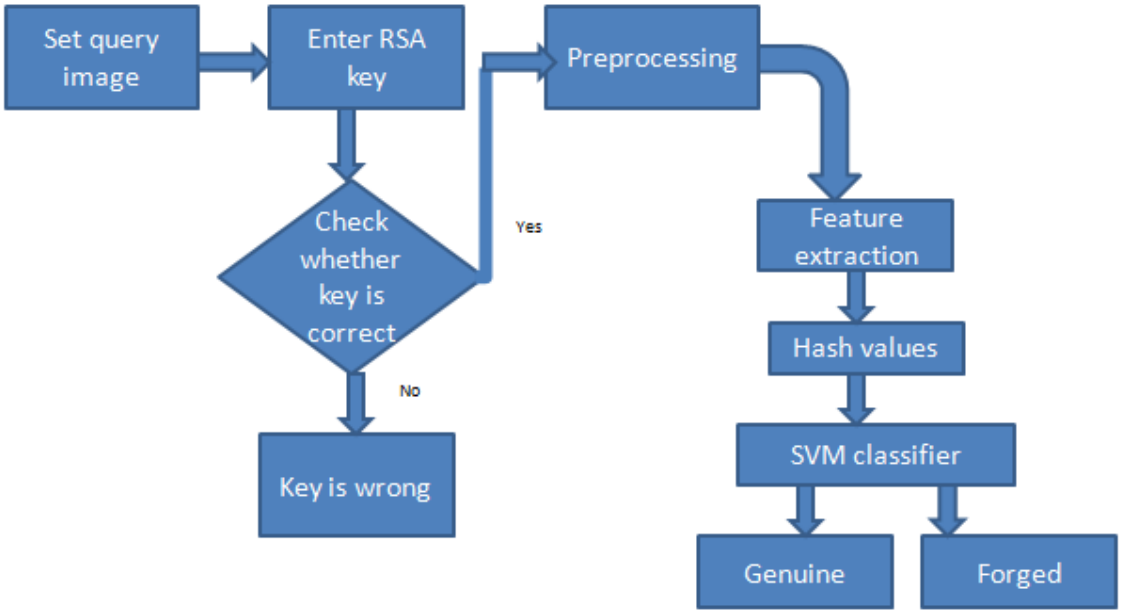

Fig.3: Testing phase

The training phase is shown in fig.3, when the query image is entered by the user, he is asked to enter the key which was set while training the database. This makes sure that the user is an authorized person. If the key is correct then image is preprocessed and features are calculated. Then the classifier classifies it as genuine image or forged.

Fig.4 (a): Original image

The original image is shown in fig.4 (a) and its manipulated image is shown in fig.4 (b) which is used as a query image.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Fig.4 (b): Query image

IV. RESULTS

The proposed method is to detect forged images. The database is created and their manipulated images are used as query image. The results for the feature calculation of original and query image are shown in table 1.The calculated hash values are shown in table 2.

	ORIGINAL IMAGE	QUERY IMAGE
MEAN	1.158780e+002	1.150377e+002
STANDARD DEVIATION	6.241583e+001	6.267167e+001
ENERGY	1.292339e-001	1.287974e-001
CORRELATION	3964	3950
VARIANCE	25	25
ENTROPY	-1	-1

Table 1: Feature extraction

The features calculated are mean, standard deviation, energy, correlation, variance and entropy. These values are converted into hash values which are shown below.

	ORIGINAL IMAGE	QUERY IMAGE
MEAN	134	132
STANDARD DEVIATION	38	39
ENERGY	0	0
CORRELATION	125	56
VARIANCE	6	6
ENTROPY	0	0

Table 2: Hash values

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Fig.5: SVM output

In this paper accuracy of detecting forgery is enhanced by using SVM classifier. For the above images taken the SVM output showed that the query image is forged. Matlab is used since all of the algorithms are coded in Matlab. All images are converted into grayscale since it is simpler to handle.

V. CONCLUSIONS

In this paper a simple method is developed for detecting the image forgery. There are training phase and testing phase. The features are extracted. The features are image, texture and pixel based. SVM classifier is trained and used to classify the query image as genuine or forged. SVM performs well on data sets that have many attributes. There is no upper limit on the number of attributes; the only constraints are those imposed by hardware. RSA key is set after training so that only authorized person can run the application to verify the authenticity of query image.

REFERENCES

[1] Sahar Q. Saleh, Muhammad Hussain, Ghulam Muhammad, and George Bebis, "Evaluation of image forgery detection using multiscale weber local descriptors," ISVC 2013, Part II, LNCS 8034, pp. 416–424, 2013.

[2] K.Shanmugapriya, M.Soniya, "An adaptive neural network classified based image forgery detection," IJAREEIE, Vol.2,Issue 12,December 2013.

[3] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, "Robust hashing for image authentication using Zernike moments and local features," *IEEE transactions on information forensics and security*, Vol. 8, No. 1, January 2013.

[4] Nitin Khanna, George T. C. Chiu, Jan P. Allebach, Edward J. Delp, "Scanner Identification with Extension to Forgery Detection," *National ScienceFoundation.*

[5] M .Sridevi, C.Mala and S.Sandeep "Copy – move image forgery detection", Computer Science & Information Technology (CS & IT) , Vol. 52 pp. 19–29, 2012.

[6] W. Luo, J. Huang, and G. Qiu, "Robust Detection of Region-Duplication Forgery in Digital Image," 18th International Conference on Pattern Recognition (ICPR'06), pp. 746-749, 2006.

[7] Junfeng He, Zhouchen Lin, LifengWang, and Xiaoou Tang," Detecting Doctored JPEG Images Via DCT Coefficient Analysis", LNCS, pp. no. 423-435, Springer, 2006.