Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.90 – 96

Detection of Image Forgery Using Color Moments and XOR Technique for Image Forensics

Apoorva Tipre, Riddhi Vadher, Nileshwari Vispute, Rozy Singh
Computer Department, Savitribai Phule Pune University, Nasik, India
hiapoorva2105@gmail.com, rvadher71@gmail.com, nileshwarivispute@gmail.com, rozysinghrajput@gmail.com

Abstract*— *So far we know that Copy-move forgery technique is used widely in the industry which includes copying part of an image and pasting it on other region of the same image. The system uses three color moments to extract feature vectors from the blocks. It is assumed that color distribution of block cannot be changed even if it compressed or blurred. Color moment is used for detection of image forgery. Next method is XOR comparison between two images for detecting forgery of images .determinant of 33 pixels is used for more performance instead of comparing pixel by pixel. Euclidean of pixel is computed to reduce dimensions from RGB vectors. This method is used to detect post processing operations and forged regions in the image with higher accuracy ratio by using color moments technique.

Keywords*— *Color Moments, XOR technique, N-Cut algorithm, Hessian matrix

I. INTRODUCTION

Today, a digital camera is used by everyone. Billions of digital images are captured. Digital images can be used in many fields such as crime investigation, journalism, medical applications. But these digital images can be easily tampered or edited with4 the help of various softwares. Forged images are used in over-advertisement, hiding facts, misunderstanding, etc which effect reputation of the victim. Authenticity of the images must be ensured because the images can be used in making critical decisions in medicine, or as an evidence in courtroom. Thus, developing image forensic methods, which deals with authenticity of images, of prime importance. Copy-move forgery is the most common type of image forgery techniques. The first method for detecting copy move forgery was proposed by Fridrich et al. in 2003[1]. Their method divides the image into overlapping square blocks. Discrete Cosine Transform (DCT) is used to extract feature vectors from the block. The quantized DCT coefficients are used to relocate similar blocks closer and then checks whether the neighbouring vectors are similar. However the method is sensitive to noise. In 2004, Popescuet al. used PCA to extract feature vectors from the blocks[2]. In 2011, Huang et al. improved the performance of the Fridrich's method by reducing the dimension of feature vector [4]. Here in this paper we are using two methods, Color moments and XOR techniques as feature extraction method to detect the copy move forgery. Color moments are mainly used for coloring indexing purposes in image retrieval applications in order to compare two similar images. Color moments are used to extract features from the overlapping blocks of the image. It divides image into overlapping blocks. The first three color moments and entropy are calculated for each block to determine the corresponding feature vector. The vectors are sorted lexicographically to make similar vectors closer. The similarity among the blocks gives a clue about forgery. It is used to differentiate images based on their colour distribution. The proposed method can detect forgery operation with acceptable accuracy ratios. It detects forged areas even if the image is post processed with some operations like Gaussian blurring and JPEG compression. However, image forgery detection has a limitation in time processing, as some method use pixel by pixel for comparison. Thus the paper proposes the method for detection of image forgery from XOR between two images and determinant of 3x3 pixels are compared. The rest of the paper is organized as follows.

II. RELATED WORK

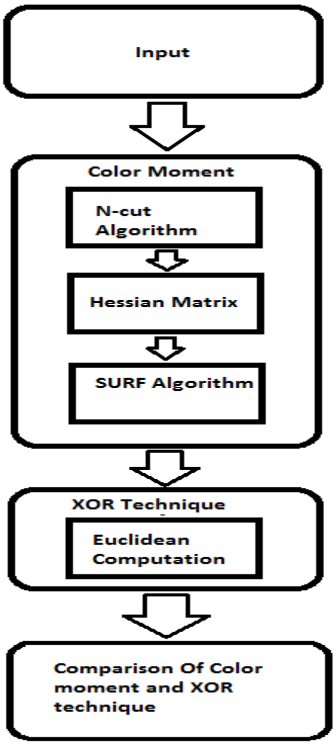
J.Fridrich et al. [1], proposed the first method for copy move forgery. With the intent to cover an important image feature, we use a special type of digital forgery, the copy move attack. Here a part of an image is copied and pasted somewhere else in the image. The forged parts are successfully detected even when the copied area is enhanced/retouched to merge it with the background and when the forged image is saved in a lossy format, uch as JPEG. But the method was sensitive to noise. In 2004, Popoescuet al.[2] used PCA to extract feature vectors from the block. The system automatically detects duplicated regions in a digital image by applying a principal component analysis to small fixed size image blocks to yield a reduced dimension representations. Due to additive noise or lossy compression, the obtained representation is robust to minor variations in the image. Lexicographical sorting is used to detect duplicated regions of images. We show the efficiency of this technique on credible forgeries, and quantify its robustness and sensitivity to addictive noise and lossy JPEG compression. In 2011, Y.Huang et al.[4] improved the performance of the Fridrich's method by reducing dimension of feature vector. Here the color image is converted from RGB color space to YCbCr color space and then overlapping blocks of fixed size are obtained by splitting R,G,B and Y-component and features are extracted image blocks on one hand and on the other, from the DCT representation of the R,G,B and Y component image block. The feature vector obtained are then lexicographically sorted to make similar image blocks neighbors and Euclidean distance formula is used as similarity criterion to find duplicated image. Experimental results showed that the proposed method can detect the duplicated regions when there is more than one copy move forged area in the image Li et al. employed Singular Value Decomposition(SVD) to decompose the low frequency sub band of the image [3]. This system uses statistical moments and two dimensional Discrete Cosine Transform (DCT). A window centered slides around every pixel of the suspicious image, the quantized coefficient matrix is obtained by passing each window through two dimensional discrete transform (2D DCT). The low dimensional statistical feature vector of each quantized coefficient matrix is obtained and arranged in A feature matrix F is consists of low dimensional statistical feature vector of each quantized coefficient matrix. The columns of F contain 4 statistical features, i.e. , mean Me, variance Var, third order moment skewness S k and the quantized coefficient matrix is used to obtain fourth order moment kurtosis Kr . Using radix sort,the feature matrix F is lexicographicaly sorted, in order to make similar windows adjacent. The adjacent pairs of feature vectors are used to perform copy-move forgery. The proposed method has the lower dimension feature vector with lower computational complexity.

III. SYSTEM ARCHITECHTURE

This paper presents the methodology for detection of Copy move forgery. Firstly, we collected set of images containing original as well as forged image. Secondly, we applied color moment algorithm which includes segmentation of image using N-cut Algorithm ,finding keypoints of segments and the original image using Hessian Matrix and then features were extracted using SURF Algorithm. Color moment Algorithm detects the copy move forgery. After that we implemented XOR technique to determine copy move forgery on the same dataset which includes pixel by pixel mapping using Euclidean Computation. Then both the Algorithms were compared

A. Data Base

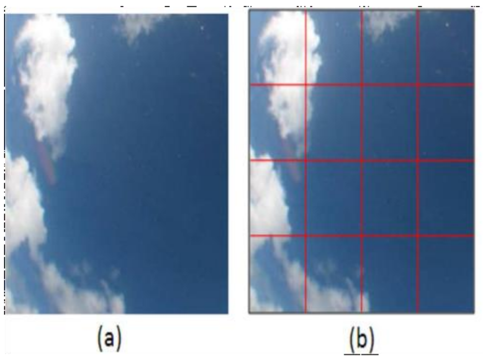
We used CoMoFoD database for a copy-move forgery detection which consist of 260 forged image sets in two categories (small 512x512, and large 3000x2000). Images were grouped in 5 groups according to applied manipulation: translation, rotation, scaling, combination and distortion. We then applied post processing methods, such as JPEG compression, blurring, noise adding, color reduction etc. to all forged and original images. Database containing images is generated.



B. Color Moment Algorithm

This consists of : N-cut algorithm , hessian matrix generation and feature vector generation using SURF Algorithm.

1) *N-cut Algorithm*: This step does the segmentation of the image into particular number of parts. The precision of this step affects the final results as only after this, we can implement the further steps. This enhances the accuracy of the result as each segment is compared with the original image.Following figure illustrates N-cut algorithm :



2) *Hessian matrix generation*: The Hessian matrix is a square matrix of second-order partial derivatives of a scalar=valued function, or scalar field. Using hessian matrix we find the keypoints of the segments of the image and the image as whole. Following matrix represents the Hessian matrix H of f is a square n×n matrix,

$$\mathbf{H} = \begin{bmatrix} \dfrac{\partial^2 f}{\partial x_1^2} & \dfrac{\partial^2 f}{\partial x_1\,\partial x_2} & \cdots & \dfrac{\partial^2 f}{\partial x_1\,\partial x_n} \\ \dfrac{\partial^2 f}{\partial x_2\,\partial x_1} & \dfrac{\partial^2 f}{\partial x_2^2} & \cdots & \dfrac{\partial^2 f}{\partial x_2\,\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{\partial^2 f}{\partial x_n\,\partial x_1} & \dfrac{\partial^2 f}{\partial x_n\,\partial x_2} & \cdots & \dfrac{\partial^2 f}{\partial x_n^2} \end{bmatrix}.$$

3) *SURF Algorithm*: A feature vector is an n-dimensional vector of numerical features that represent some object. A feature vector for each segment is calculated.

C. XOR Technique

XOR/Exclusive-OR is a logic operator where the output is 1 if input are different value. And the output is 0 if input are the same value. In this pixel by pixel mapping of the image is done by measuring Euclidean distance. A pixel consist of many variables. Euclidean is used to decrease dimensionality of variables. Euclidean is used as a normalized representative value for RGB of a pixel using following formula

$$\|r, g, b\| = \sqrt{r^2 + g^2 + b^2}$$

D. Comparison

The results of color moment Algorithm and XOR technique is compared here.
A threshold is set for the comparison of both the techniques and accordingly it is decided which technique gives more accuracy in the result.

IV. ALGORITHM

A. Color Moments

The difference between two imagines can be obtained based on their color distribution which is known as color moments. Color moments are used for color indexing purpose as features in image retrieval applications in order to compare similarity between two images based on color. A similarity score is obtained by comparing images. The color moments are used to extract features vector from the blocks which gives color distribution of the corresponding block. The image is divided into overlapping blocks and features extracted. Feature vectors are placed into a matrix which is lexicographically sorted to make the similar vectors closer. In the second phase similar blocks are searched and calculation of shift vectors is done from each suspicious block pairs. If the number of suspicious block pairs that have the same shift vectors exceed a predetermined threshold value then those blocks are forged. The proposed algorithm framework of copy-move forgery detection. The algorithm can be given in the form of steps as below.

1) *Block Tilling*: The suspicious RGB colour image of size *MxNx3* pixels is divided into overlapping fixed size *BxB* blocks. We used *B* to be 8 in this work.

2) *Feature Extraction*: We use circle block instead of square block. The radius of the circle, *r*, is chosen to be *B/2*. To determine the feature vector, we calculate first three color moments from each color channel and corresponding entropy from this block. The moments are calculated using :

$$E_i = \sum_{j=1}^{N} \frac{1}{N} p_{ij}$$

$$\sigma_i = \sqrt{\left(\frac{1}{N}\sum_{j=1}^{N}\left(p_{ij} - E_i\right)^2\right)}$$

$$s_i = \sqrt[3]{\left(\frac{1}{N}\sum_{j=1}^{N}\left(p_{ij} - E_i\right)^3\right)}$$

The luminance value *Y* for the current pixel is calculated as,
Y=0.2126r+0.7152g+0.0722b.

The probability distribution function is calculated using the luminance value of all the pixels within a circular block. From this, entropy= $\Sigma p_k \log_2 p_k$, where p_k is the probability of each luminance value in the circular block.

The feature vector is given by

$$F = \{ E_r, \sigma_r, S_r, E_g, \sigma_g, S_g, E_b, \sigma_b, S_b, e\}$$

and the feature vector matrix is prepared.

3) *Matching Algorithm:* S is a lexicographically sorted matrix of feature vectors. The method uses a difference array to represent the distance between corresponding vector elements. Each element of the array is calculated using $Diff(k) = |F(i) - F(j)|, 1 \le k < 10$. If *Diff(k)* is smaller than a predetermined threshold *P(k)* and entropy is greater than a predefined threshold *s*, the actual distance is calculated between the blocks designated by these vectors. The distance between blocks corresponding to these vectors are calculated. If the actual distance between the inquired blocks is larger than a predefined threshold value *D*, the blocks will be labelled as candidate for the forgery. The distance between two similar blocks is calculated as follows:

$$Dist(F_i, F_{i+j}) = \sqrt{(x_i - x_{i+j})^2 + (y_i - y_{i+j})^2} >= D$$

where (x,y) is the coordinates of the circle center of the corresponding block. Shift vector is a pair, which gives absolute difference between the x coordinates and y coordinates of the corresponding blocks. Shift vector is determined for the j^{th} and $(j+1)^{th}$ block

$$(s_x, s_y) = (|(x_j - x_{j+1})|, |(y_j - y_{j+1})|)$$

4) *Judgment about the forgery:* In this step, the method evaluates the shift vectors. If the number of any shift vector exceeds a predefined threshold value *NS*, corresponding blocks, which create the shift vector, are marked as forged. Otherwise, this means that related blocks represents discrete regions and they are ignored. Last step creates an image, which has black regions to show the copy move forgery.

B. XOR Technique

Using this technique, XOR is calculated between two images and determinant of pixels. In this method, pixels of image are determined and then their neighbours are found out using first order neighbourhood system. This method can integrate with trigonometry for solving the geometric correction such as rotated images.

1) *Computation of First-order Neighbours:* Compute the representative value of 9 pixels using first-order neighbours of a pixel.

$$N^{\varpi=1}(s) = \{S_{x-1}^{y-1}, S_{x}^{y-1}, S_{x+1}^{y-1}, S_{x-1}^{y}, S_{x+1}^{y}, S_{x-1}^{y+1}, S_{x}^{y+1}, S_{x+1}^{y+1}\}$$

S_{x-1}^{y+1}	S_{x}^{y+1}	S_{x+1}^{y+1}
S_{x-1}^{y}	S_{x}^{y}	S_{x+1}^{y}
S_{x-1}^{y-1}	S_{x}^{y-1}	S_{x+1}^{y-1}

2) *Euclidean Computation:* A pixel has many variables. Euclidean is used to decrease dimensionality of variables. Each pixel consists of the red value, green value and blue value. Euclidean is used as a normalized representative value for RGB of a pixel.

$$\|r,g,b\| = \sqrt{r^2 + g^2 + b^2}$$

3) *Determinant Computation:* Compute the determinant of 9 pixels to find the representative of the pixel values;

$$\text{Define } A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

4) *XOR Comparison between two images:* XOR is used to compare the determinant of pixels between forged image and real image.

V. PERFORMANCE ANALYSIS

We are implementing the system using JDK 1.8. We used the latest version of Eclipse IDE platform for implementation. All the algorithms were run using device having Intel(R) Core(TM) i5-5250U CPU @ 1.60 GHz with 8 GB RAM and Windows 10 operating System. We took 500 images from the dataset. Database is created using Xaamp 5.6.23 in which MYSQL is used.

VI. CONCLUSION

This project focuses on methods to detect digital forgeries created from portions copied and moved within the same image to cover-up something are called as copy-move forgeries. Hessian features and XOR technique is use to detect a passive copy-move image forgery. The proposed method not only detects the simple one to one copy move forgery but also performs well when certain post processing operations such as adding noise, image compression, blurring, rotation, scaling or any composite operations which are applied to makes the detection complicated.

REFERENCES

[1] J. Fridrich, Detection of copy-move forgery in digital images, Digital Forensic Research Workshop, Cleveland, OH, 2003, pp. 1923

[2] J. A. C. Popescu, H. Farid, Exposing digital forgeries by detecting duplicated image regions, Tech. Rep. TR2004-515.

[3] Q. T. D. S. S. Li, G. Wu, A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, ICME, 2007

[4] S. Bayram, H. Sencar, N. Memon, An e_cient and robust method for detecting copy-move forgery, IEEE International Conference on Acoustics, Speech and Signal Processing, 2009, pp.

[5] Y. Huang, Improved DCT-based detection of copy-move forgery in images, Forensic Science International, 206(1-3), 2011, pp. 178-184

[6] P. Yadav, "Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform" Department of Computer Science and Engineering", CSVTU, 2012.