International Journal of Engineering Research and General Science Volume 3, Issue 3, Part-2 , May-June, 2015
ISSN 2091-2730

Image Authentication and Forgery Localization

Dinu Innocent, Gopakumar G, Neethu Treesa Jacob

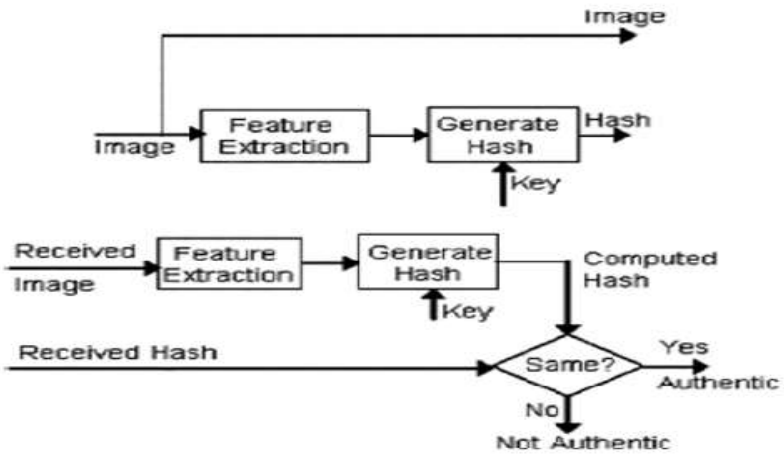
CUSAT university, dinuinnocent@gmail.com, +91 8157044109

Abstract— Robust hashing method is developed for detecting image forgery including removal, insertion, and replacement of objects, and abnormal color modification, and also copy move and spliced forgery, and for locating the forged area. Both global and local features are used in forming the hash sequence. The global features are based on Zernike moments representing luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image. Secret keys are introduced in feature extraction and hash construction. While being robust against content preserving image processing, the hash is sensitive to malicious tampering and, therefore, applicable to image authentication. The hash of a test image is compared with that of a reference image. When the hash distance is greater than a threshold T1 and less than T2, the received image is judged as a fake. By decomposing the hashes, the type of image forgery and location of forged areas can be determined e.g., replacement of objects or abnormal modification of colors or copy move and spliced forgery. Compared with some other methods using global features or local features alone, the proposed method has better overall performance in major specification, especially the ability of distinguishing regional tampering from content preserving processing.

Keywords— image hashing, Zernike moments, salient region, global and local feature, splicing, Speeded Up Robust Features, Local Binary Pattern,

INTRODUCTION

With the widespread use of image editing software, ensuring credibility of the image contents has become an important issue. Image hashing is a technique that extracts a short sequence from the image to represent its contents, and therefore can be used for image authentication .If the image is maliciously modified, the hash must be changed significantly. Below figure shows the concept of image hashing.



A good image hash should be reasonably short, robust to ordinary image manipulations, and sensitive to tampering. It should also be unique in the sense that different images have significantly different hash values, and secure so that any unauthorized party cannot break the key and coin the hash. To meet all the requirements simultaneously, especially perceptual robustness and sensitivity to tampering, is a challenging task.

So many techniques are introduced with Image Hashing Development. Image hash is developed as a result of feature extraction and the coding of intermediate result. That has become a routine practice in many image hashing methods. Many previous schemes are either based on global [2]-[5] or local [6]-[8] features. Global features are generally short but insensitive to changes of small areas in the image, while local features can reflect regional modifications but usually produce longer hashes.

The proposed method combines the advantages of both global and local features. The objective is to provide a reasonably short image hash with good performance, i.e., being perceptually robust while capable of detecting and locating content forgery. We use Zernike moments of the luminance/chrominance components to reflect the image's global characteristics, and extract local texture features from salient regions in the image to represent contents in the corresponding areas. Distance metrics indicating the degree of similarity between two hashes are defined to measure the hash performance. Two thresholds are used to decide whether a given image is an original/normally-processed or maliciously doctored version of a reference image, or is simply a different image. The method can be used to locate tampered areas and tell the nature of tampering, e.g., replacement of objects or abnormal modification of colors. Compared with some other methods using global features or local features alone, the proposed method has better overall performance in major specifications, especially the ability of distinguishing regional tampering from content preserving processing. The previous scheme [1] only considers forgeries like replacement of objects or abnormal modification of colors addition or removal of object. But the proposed method can found out other two main forgeries such as copy move forgery and spliced attack.

PROPOSED METHOD

The proposed method combines the advantages of both global and local features. The objective is to provide a reasonably short image hash with good performance, i.e., being perceptually robust while capable of detecting and locating content forgery.Here use Zernike moments of the luminance/chrominance components to reflect the image's global characteristics, and extract local texture features from salient regions in the image to represent contents in the corresponding areas. Distance metrics indicating the degree of similarity between two hashes are defined to measure the hash performance. Two thresholds are used to decide whether a given image is an original/normally-processed or maliciously doctored version of a reference image, or is simply a different image. The method can be used to locate tampered areas and tell the nature of tampering, e.g., replacement of objects or abnormal modification of colors. Compared with some other methods using global features or local features alone, the proposed method has better overall performance in major specification, especially the ability of distinguishing regional tampering from content-preserving. The proposed method can found out other two main forgeries such as copy move forgery and spliced attack other than the normal forgeries such as replacement of objects or abnormal modification of colors addition or removal of object.

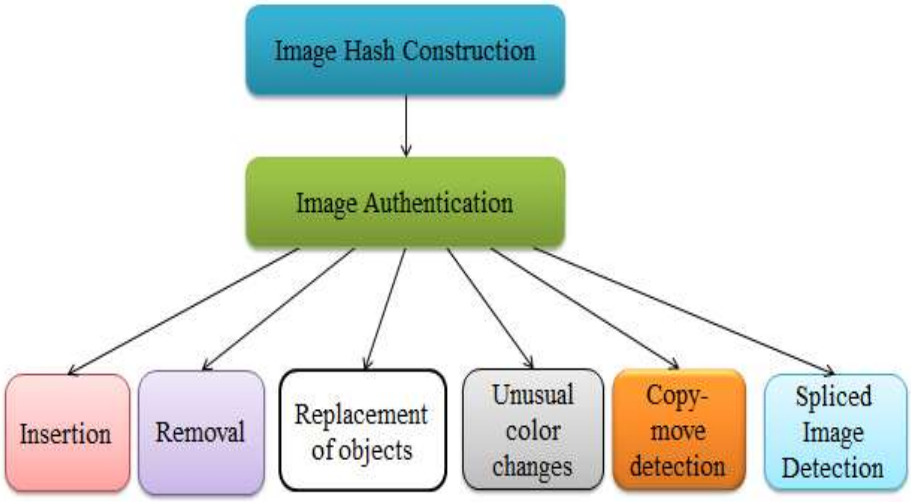
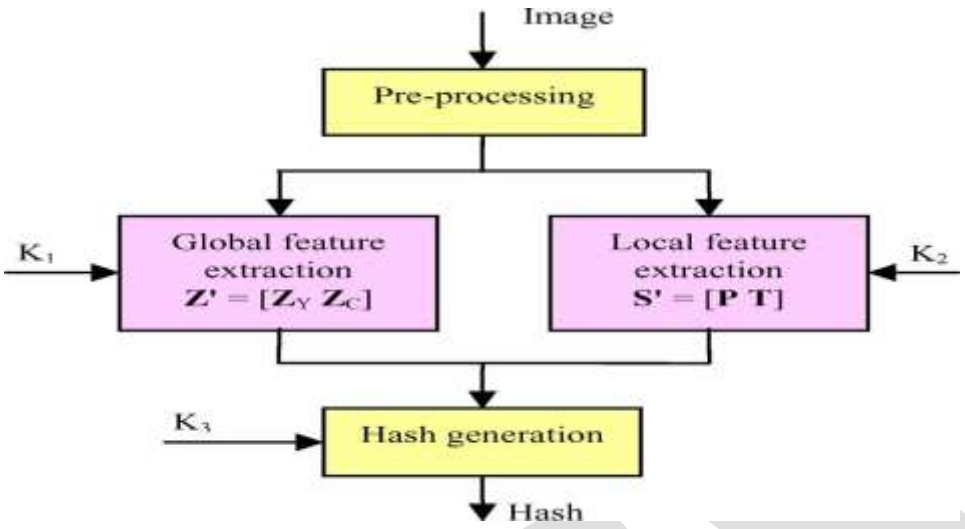


IMAGE HASH CONSTRUCTION

Proposed hashing scheme uses the global and local feature extraction for the construction of image hash for the authentication process.The global vector is 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.



Preprocessing:

The image is first rescaled to a fixed size FxF with bilinear interpolation, and converted from RGB to the YCbCr representation and |Cb-Cr| are used as luminance and chrominance components of the image to generate the hash. The aim of rescaling is to ensure that the generated image hash has a fixed length and the same computation complexity. Small F leads to loss of fine details, while large F results in high computation complexity. Here choose F=256 as an appropriate trade-off.

Global Feature Extraction:

Zernike moments of Y and |Cb-Cr| are calculated.Zernike moments (ZMs) have been used in object recognition and image analysis regardless of variations in position, size and orientation. Basically, the Zernike moments are the extension of the geometric moments by replacing the conventional transform kernel with orthogonal Zernike polynomials.

Zernike moments(ZM)of order n and repetition m of a digital image $I(\partial,\theta)$can be find out using the below algorithm:

a) Select the values for order n and the repetition m such that, n=0,1..... , 0<=|m|<=n and n-|m| is even.

b) Calculate the Zernike Polynomial of order ”n‟ and repetition “m‟.

$$Vnm(\rho, \theta) = Rnm(\rho)e^{jm\theta}$$

Where Rnm(ρ) are real-valued radial polynomials

$$R_{nm}(\rho) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!}\rho^{n-2s}.$$

Where ρ=length of vector from origin to a pixel, θ=angle between vector and x axis.

c) Multiply the digital image with the Zernike Polynomial.

d) Take the summation over the entire image.

$$Z_{n,m} = \frac{n+1}{\pi} \sum_{(\rho,\theta)\in \text{unit disk}} \sum I(\rho,\theta) V^*_{n,m}(\rho,\theta)$$

Because shape features can be obtained from a small number of low frequency coefficients, the order does not need to be large. This method choose n=5. For n=5, we have 11 Zernike moments, so total 11*2=22 integers. (For luminance and chrominance components) as in the table.

ZERNIKE MOMENTS OF DIFFERENT ORDERS

Order n	Zernike moments	Number of moments
1	$Z_{1,1}$	1
2	$Z_{2,0}$, $Z_{2,2}$	2
3	$Z_{3,1}$, $Z_{3,3}$	2
4	$Z_{4,0}$, $Z_{4,2}$, $Z_{4,4}$	3
5	$Z_{5,1}$, $Z_{5,3}$, $Z_{5,5}$	3

Magnitudes of the Zernike moments are rounded and used to form a global vector, $Z^{'}$=[Zy , Zc] .Each element in is no more than 255.A secret key K1is used to randomly generate a row vector X1with 22 random integers in [0, 255]. The encrypted global vector Z is obtained as Z= [($Z^{'}$+X1) mod 256]

Local Feature Extraction:

The coordinates of top left corner and width/height of each salient region in an image and some texture features are used as the local feature.

A salient region in an image is one that attracts visual attention. According to [11], information in an image can be viewed as a sum of two parts: that of innovation and that of prior knowledge. The former is new and the latter redundant. The information of saliency is obtained when the redundant part is removed. Log spectrum of an image, L (f), is used to represent general information of the image. Because log spectra of different images are similar, there exists redundant information in L (f).

The Salient Region can be detected using the algorithm

a) Calculate the log spectrum of the image, L (f)

b) Find the redundant information exists in the image.

A (f) =h1*L (f) h1=low-pass kernel

c) Obtain the spectral residual by subtracting redundant information from the log spectrum of the image.

B (f) =A (f)-L (f)

d) Calculate the saliency map by inversely Fourier transforming the spectral residual.

Sm(x) =F` (B (f))

e) Determine the salient regions by

O(x) = 1 if S(x) > threshold,

0 otherwise.

Threshold = E(S(x)) × 3, where E(S(x)) is the average intensity of the saliency map.

Fig. 1. Salient region detection: (a) Original image. (b) Saliency map. (c) Salient region. (d) Four rectangles.

K largest salient regions are detected from the luminance image Y. The coordinates of top left corner, and width/height of each circumscribed rectangle are used to form a K element vector P^k, representing the position and size of each salient region. With a larger K, fewer salient regions are missing but will lead to a longer image hash. Also the percentage of images with no more than 7 salient regions is 99.5%.This method choose K=6 as a reasonable trade-off.

Texture Features

Texture is an important feature to human visual perception.There is mainly six texture features relating to visual perception: coarseness, contrast, directionality, line-likeness, regularity and roughness. Here uses coarseness C_1 and contrast C_2 as defined below, plus skewness and kurtosis, to describe the texture properties. Skewness and kurtosis can be obtained by histogram representation.

The algorithm used to find the Coarseness around a pixel is:

a) Select a pixel at (x , y).

b) Averaging the 2k x 2k neighborhood pixels of the above selected pixel.

$$A_k(x,y) = \frac{1}{2^{2k}} \sum_{i=x-2^k}^{x+2^k-1} \sum_{j=y-2^k}^{y+2^k-1} g(i,j), \quad k = 0, 1, \ldots, 5$$

c) Find the average values of non overlapping neighborhoods on opposite sides of the selected pixel in horizontal and vertical directions.

d) Calculate the difference between the pairs of average values.

$$E_{k,h}(x,y) = |A_k(x + 2^{k-1}, y) - A_k(x - 2^{k-1}, y)|$$
$$E_{k,v}(x,y) = |A_k(x, y + 2^{k-1}) - A_k(x, y - 2^{k-1})|$$

e) Find the size that leads to the highest difference value.

$$S_{\text{opt}}(x,y) = \underset{k=0,\ldots,5;d=h,v}{\arg\max} E_{k,d}(x,y)$$

f) Take average on the highest difference value over a region in order to obtain Coarseness.

Contrast is obtaining the algorithm:

a) Calculate the variance of the gray values of the image.

b) Calculate the fourth order moment of the gray values of the image.

c) Multiply the calculated variance and the fourth-order moment within the region.

$$C_2 = \sigma^2 \mu_4^{-4}$$

So local vector is the combination of position value P (x, y, height, width) and texture features T. position vector P contains 6*4=24 integers also texture feature vector contain 6*4=24 integers, since we consider 6 salient region.So local feature vector contain 48 integers.

S1= [P, T]

S= [(S1+X2) mod 256] where X2 is the row vector generated using a secret key K2.

Hash construction:

The global and salient local vectors are concatenated to form an, intermediate hash H1= [Z, S] scramble H1 based on a key K3 to produce the final hash sequence H.

H= [(H1+X3) mod 256] where X3 is the row vector generated using a secret key K3.

So total our image hash contain 24+24+22=70 integer and is 70*8=560bits long.

IMAGE AUTHENTICATION

In image authentication, the hash of a trusted image H_0 is available and called the reference hash. The hash of a received image to be tested H_1 is extracted using the above method.

a) The hash of a received image to be tested (H_1) is extracted.
H_1= [Z1 P1 T1]

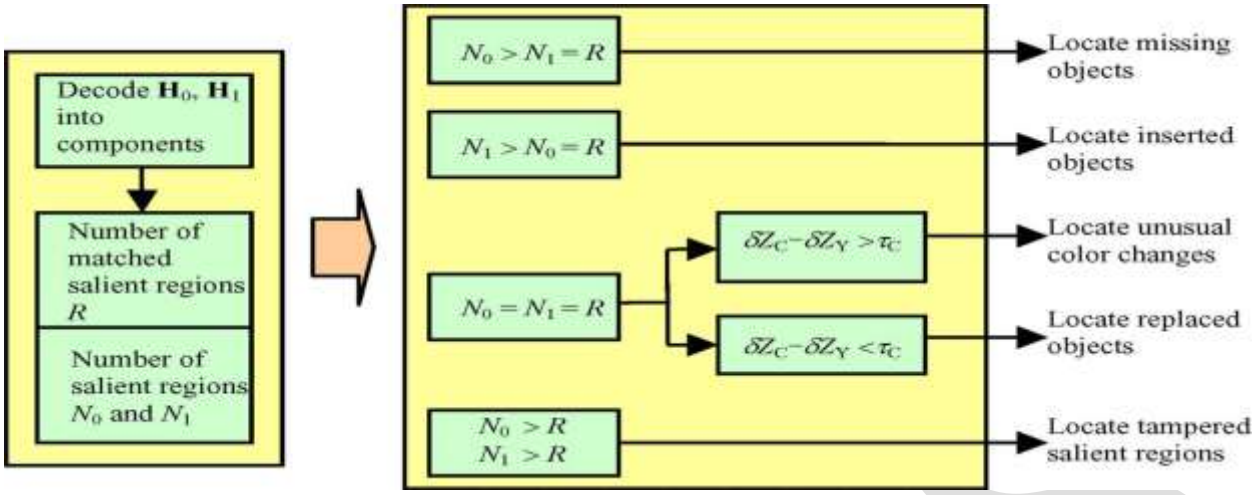
b) Decompose the reference hash (H0) into Global and Local features.
H_0= [Z0 P0 T0]

c) Check if the salient regions found in the test image P1 match those in the trusted image P0.

These two hashes are compared to determine whether the test image has the same contents as the trusted one or has been maliciously tampered, or is simply a different image. Here, two images having the same contents (visual appearance) do not need to have identical pixel values. One of them, or both, may have been modified in normal image processing such as contrast enhancement and lossy compression. In this case, we say the two images are perceptually the same, or similar.

FORGERY CLASSIFICATION

Forgery classification includes classifying the possible forgeries as removal, insertion and replacement of objects, and unusual color changes. For that, Decode H_0 (hash of the test image) and H_1 (hash of the reference image) into components representing global and local features, and find the number of matched salient regions R and the numbers of salient regions in the reference N_0 and test images N_1 then check some conditions which is described below.



$$\delta Z_C = ||\mathbf{Z}_{C1} - \mathbf{Z}_{C0}||, \quad \delta Z_Y = ||\mathbf{Z}_{Y1} - \mathbf{Z}_{Y0}||$$

The method for finding other two forgeries like copy move and spliced forgery are described below.

COPY MOVE FORGERY

A copy move forgery denotes an image where part of its content has been copied and pasted within the same image. Typical motivations are either to hide an element in the image, or to emphasize particular objects.Here key point-based method is used. In key point-based method, SURF (Speeded Up Robust Features) method is used for feature extraction. Key point-based methods compute their features only on image regions with high entropy, without any image subdivision for feature extraction. Similar features within an image are afterwards matched.

Algorithm for detecting copy move forgery is given below.

A. Pre-Processing:

Here the image is converted from RGB to Gray representation.

B. Feature Extraction:

The features can be extracted by using SURF (Speeded Up Robust Features) method. SURF is the robust local feature detector. Shape feature used to locate and recognition of certain objects, people or faces, object tracking and extraction of points of interest.

C. Matching:

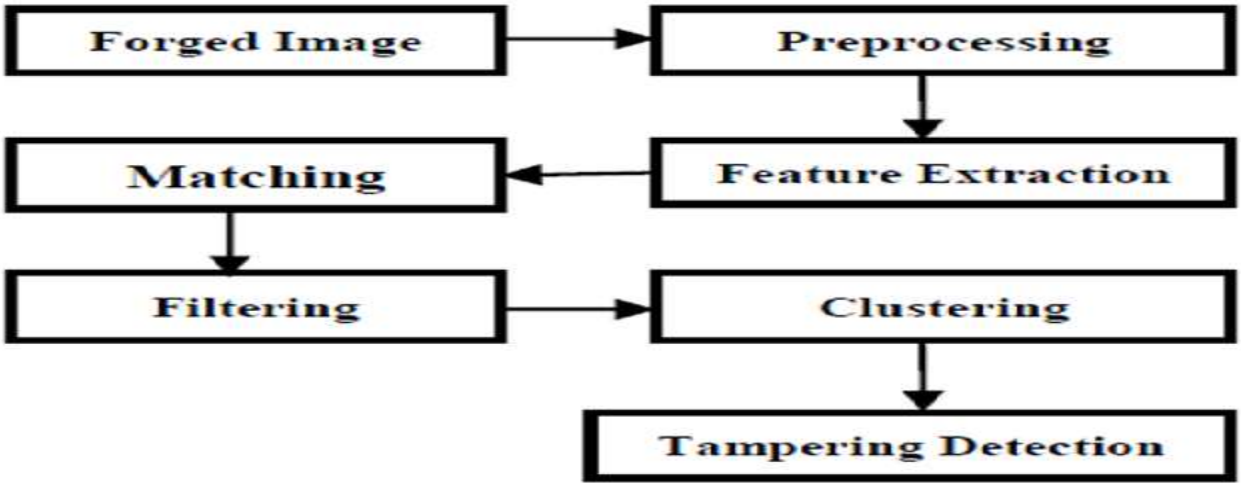
A matching operation is performed among the feature vectors to identify similar local patches in the image. Approximate Nearest Neighbor method is used for feature matching.

D. Filtering:

Filtering schemes are used to reduce the probability of false matches. Neighboring pixels often have similar intensities, which can lead to false forgery detection. The Euclidean distance that can be calculated between each feature vectors. The pairs can be removed if it is less than the particular threshold value T2.

E. Clustering:

The Agglomerative Hierarchical Clustering is used to cluster the forged regions.



SPLICED FORGERY

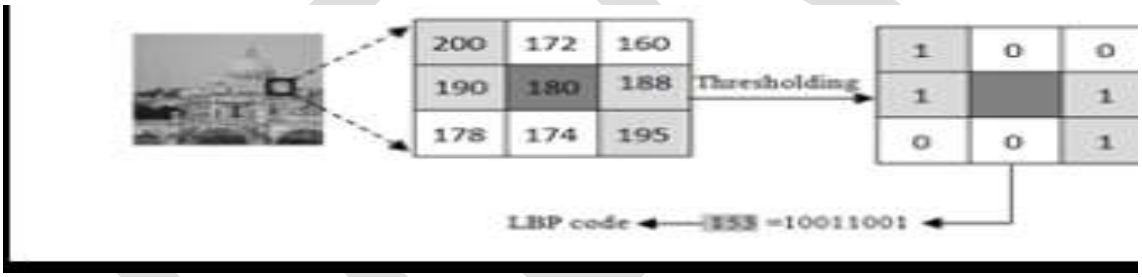
Simple joining of fragments of two or more different images leads to the splicing attack.

A. Preprocessing

Input RGB color image is transformed to YCbCr color system. Chrominance component (Cb or Cr) is divided into 16x16 overlapping blocks.

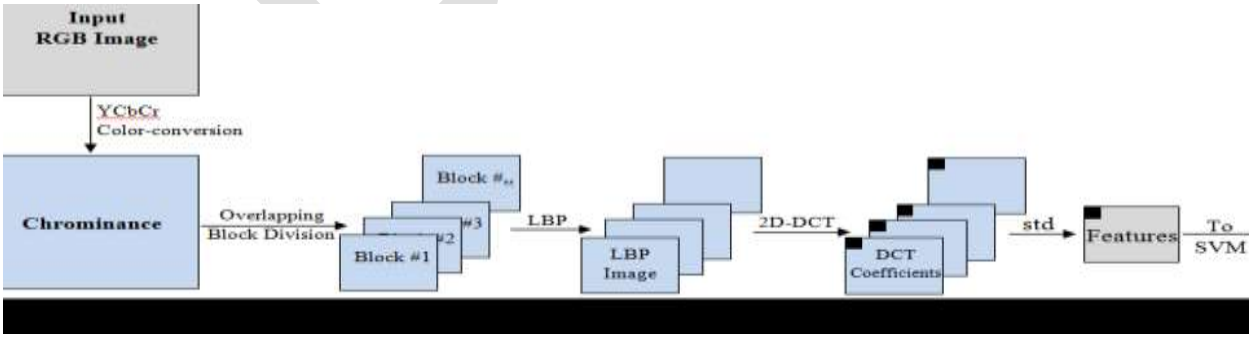
B. Local Binary Pattern (LBP)

LBP is a local operator which discriminates different types of textures and defines a label (LBP code) of each pixel of an image. To compute the LBP code, a 3x3 neighborhood of the pixel is threshold by its intensity value. If the neighbor's pixel value is less than the center, it will hold binary digit '0', otherwise it will hold '1'.The neighbors' binary digits are concatenating to build a binary code. The LBP code is the decimal value of that binary code. Calculated LBP is transformed into frequency domain using 2D DCT. Then standard deviations are calculated of respective frequency coefficients of all blocks and they are used as features.



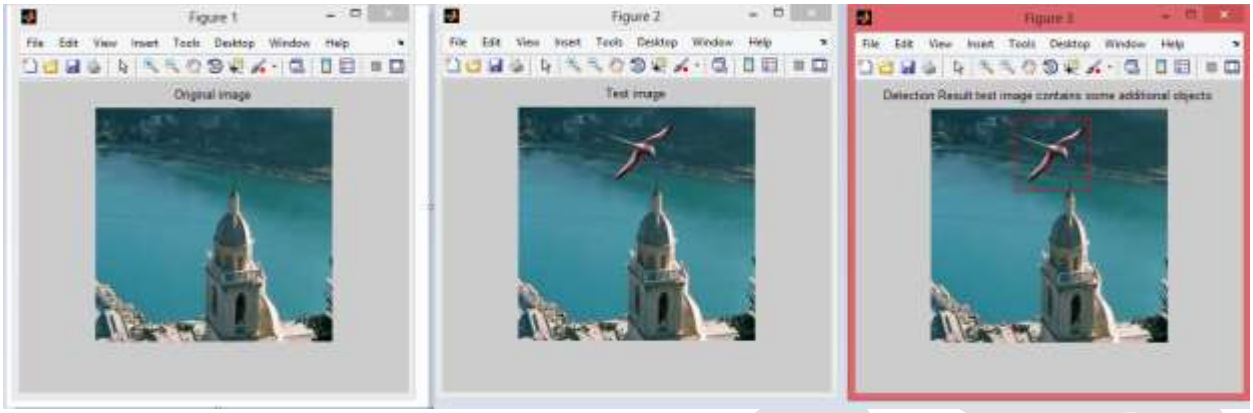
C. Classification

Finally, these features are sent to SVM classifier in order to make the decision about the input image whether it is an authentic or a tampered one.

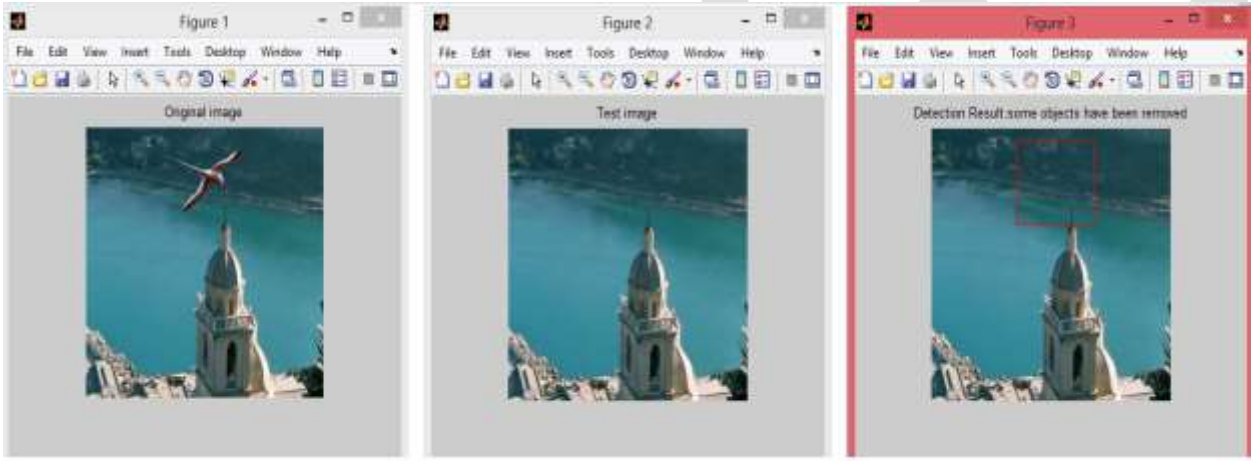


RESULTS

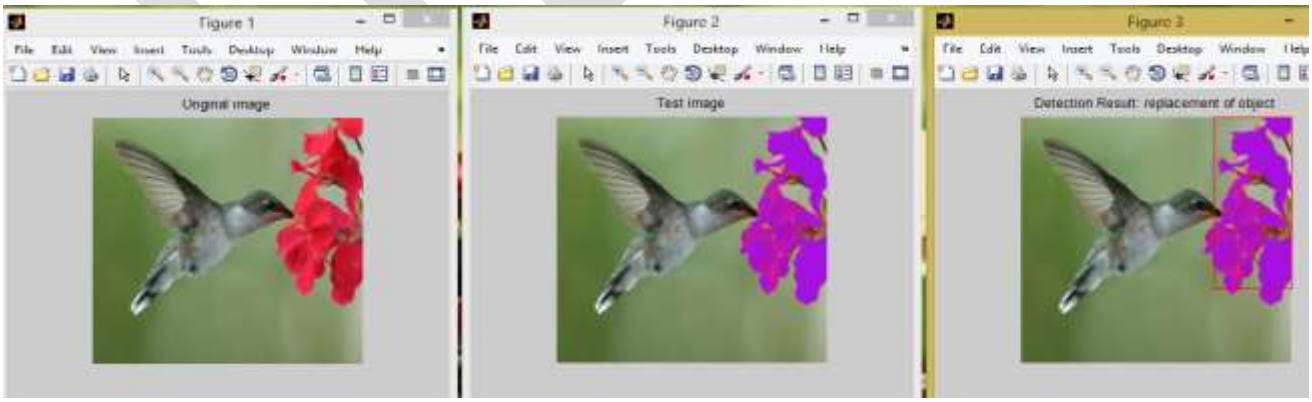
1. Addition of object



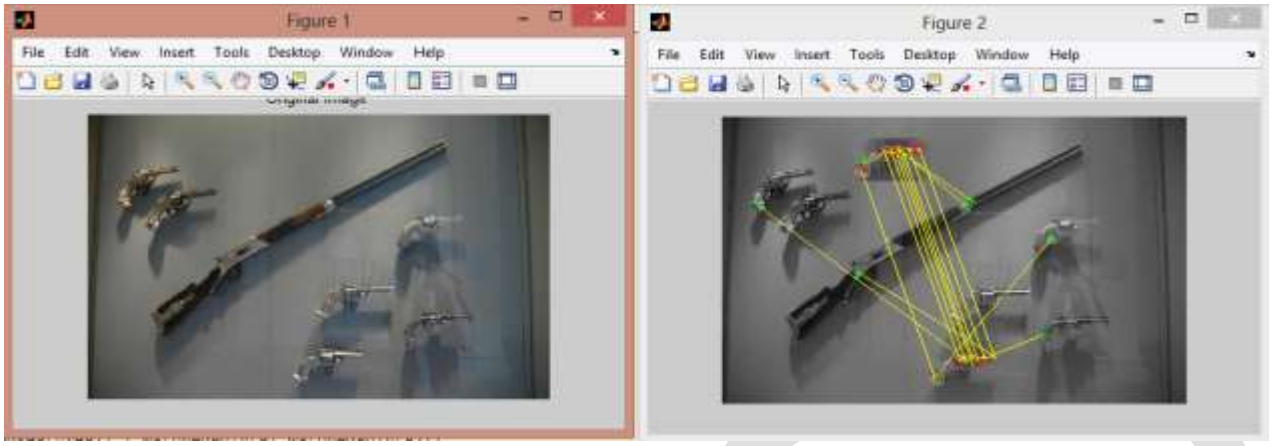
2. Removal of object



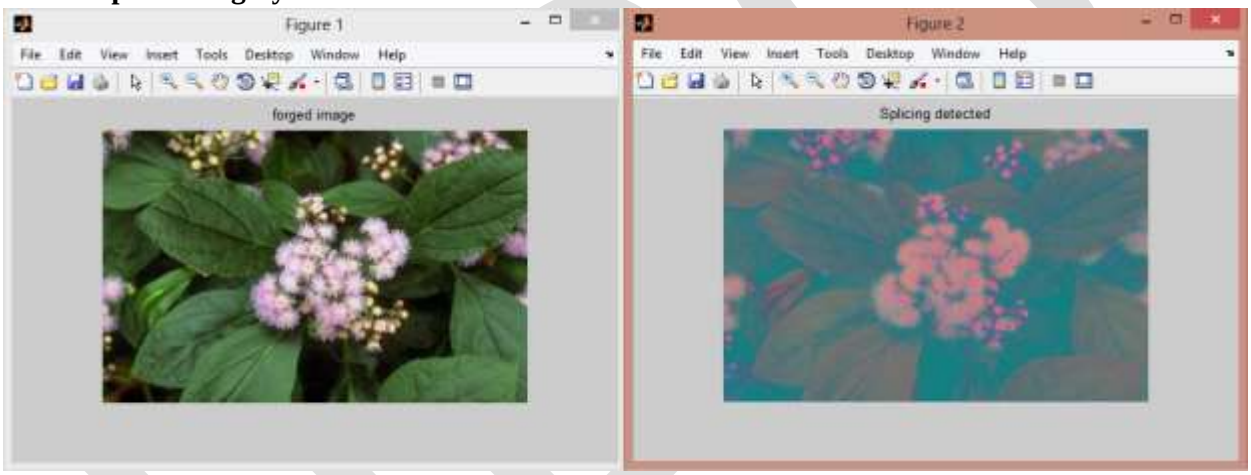
3. Replacement of object



4. Copy move forgery



5. Spliced forgery



CONCLUSION

In this work, 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.

Hashes produced with the proposed method are robust against common image processing operations including brightness adjustment, scaling, small angle rotation, JPEG coding and noise contamination. Collision probability between hashes of different images is very low. The proposed scheme has a reasonably short hash length.

The method used in this work is aimed at image authentication. The hash can be used to differentiate similar, forged, and different images. At the same time, it can also identify the type of forgery and locate fake regions containing salient contents. In the image authentication, a hash of a test image is generated and compared with a reference hash previously extracted from a trusted image. When the hash distance is greater than the threshold T_1 but less than T2 the received image is judged as a fake. By decomposing the hashes, the nature of image forgery and locations of forged areas can be determined. The previous scheme [1] only considers forgeries like replacement of objects or abnormal modification of colours addition or removal of object. But the proposed method can found out other two main forgeries such as copy move and spliced forgery.

REFERENCES:

[1] 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

[2] V. Monga, A. Banerjee, and B. L. Evans, "A clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 68–79, Mar. 2006.

[3] Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121–128.

[4] Tang, S.Wang,X. Zhang, W.Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.

[5] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp.215–230, Jun. 2006.

[6] K. Fouad and J. Jianmin, "Analysis of the security of perceptual image hashing based on non-negative matrix factorization," IEEE Signal Process. Lett., vol. 17, no. 1, pp. 43–46, Jan. 2010.

[7] W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information," in Proc. SPIE,Media Forensics and Security II, San Jose, CA, Jan. 2010, 7541.

[8] W. Lu and M.Wu, "Multimedia forensic hash based on visual words," in Proc. IEEE Conf. on Image Processing, Hong Kong, 2010, pp. 989–992.

[9] S. Li, M. C. Lee, and C. M. Pun, "Complex Zernike moments features for shape-based image retrieval," IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 39, no. 1, pp. 227–237, Jan. 2009.

[10] Z. Chen and S. K. Sun, "A Zernike moment phase based descriptor for local image representation and matching," IEEE Trans Image Process., vol. 19, no. 1, pp. 205–219, Jan. 2010.

[11] X. Hou and L. Zhang, "Saliency detection: A spectral residual approach," in Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, Minneapolis, MN, 2007, pp. 1–8.

[12] T. Deselaers, D. Keysers, and H. Ney, “Features for image retrieval: A quantitative comparison,” in *Lecture Notes in Computer Science*, 2004, vol. 3175, pp. 228–236, Springer