DOI 10.29042/2018-3741-3745

Helix Vol. 8(5): 3741- 3745

A Hashing Based Approach to Detect Object Tampering

[*1]Harshita Gour, [2]Dr. Manoj B. Chandak
[1, 2] Shri Ramdeobaba College of Engineering & Management, Nagpur, India.
**Email: [1]gourhr@rknec.edu, [2]chandakmb@gmail.com*

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract

Tampering detection techniques have been continuously studied with advancements in technologies. However, many existing alternatives cannot generate object tampering results, because of the hashes attached to the image shortfall the outline information. Object tampering detection is the process of locating the modifications in the structure of an object. In this paper, we presented a method of object tampering detection which will generate the results showing the tampered images of the object. Firstly, different images of the same object are taken from different angles. Furthermore, each image of the object will then be processed to localize the region of tampering in the object. The model estimates the parameters associated with an image such as shape hash, color hash, and hash vector. Finally, a classification system, Support Vector Machine (SVM) will classify the images as tampered or not tampered based on the input fed to the classification system. This method will be useful for the product manufactures to meet the growing demands of the product as tampered products lead to non-acceptability to the end user. This technique will reduce the manpower for quality check control of the products and will identify the tampered objects from the collection.

Keywords: Object Tampering, Shape Hash, Color Hash, Hash Vector, SVM.

Introduction

With the advancement in technologies and continuous diversified market needs, it becomes mandatory for the product manufacturers to meet the growing demands of the product with high performance in less delivery time. To meet this growing demand, a lot of control efforts are required. For a product to be effective, its quality is a major concern that can be evaluated in various parameters. Quality of the product also called as features can be measured in terms of internal and external factors. Internal quality factors include the raw material required for the manufacturing of the product whereas external quality factors concern with the finished goods. Hence to identify object tampering, we proposed a novel technique to identify the tampered regions in the product. This method will analyse different images of the object and will generate the results showing the tampering in images of the object and its location where the object has tampered. This technique will reduce the manpower for quality check control of the products and will identify the tampered objects from the collection. The widespread use of technologies and the growing market needs, it becomes necessary for the manufacturers to deliver the products with good performance and with short delivery time. Some recent work and studies based on tampering detection and hashing is discussed. [1] Chi-Man Pun, Caiping Yan, and Xiao-Chen Yuan proposed a design of Image Alignment based Multi Region Matching (IAMRM) algorithm for object level tampering detection. In this scheme, an adaptive segmentation model is used to divide an image into regions on the basis of strong edges. Color based multi region matching along with color location based multi region matching was used to locate the tampered part in the image. [2] S. M. Koon, M. H. Jakubowski, and P. Moulin, introduced the phenomenon of hashing making use of wavelet coefficients as a descriptors for the generation of hash values. This technique was proved as a robust method against any type of attack, distortion or compression. [3] D. Vats, and B. L. Evans described the characteristic feature for comparison of images in the process of image authentication but the process seemed to be of low accuracy as it becomes necessary to adjust the parameters of different images.[4] Pang, X. Zhou, Y. Zhou, L. Li, and J. Xue described an image hash method which is a combination of features based on image-block and features based on key-points This method tried accurately to locate the tampered regions properly, but the drawback emerged as the variation of hash length ranging from tens to thousand. Although various different robust alignment techniques have been suggested by the researchers [5]–[7], but the techniques became unsuitable in the terms of forensic hashing, because the fundamental property requires that image signature or the hash must be as compact as possible.. To meet the requirements, authors of [8] have suggested to exploit information derived through Radon transform and scale space theory to describe the parameters of the geometric transformations

Materials and Methods

Object tampering detection is the scheme to find out the location of modification in the structure of an object. This approach aims to find any irregularity in

the structure of object when quality factors are concerned. Also, this scheme detects the tampered part of an object when the object is about to be sold for its sale. This approach enables the classification of an object for the sale. Figure 1 shows the proposed scheme for object tempering detection using hash value extraction.

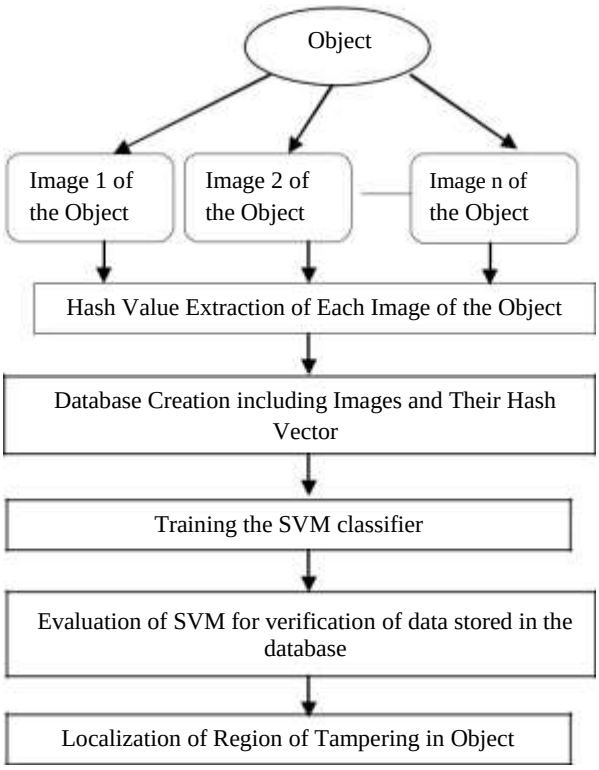

Figure 1: Flowchart of the Proposed Method

Image Characteristics

Color Hash

An RGB image is composed of three channels- red, green and blue. If the RGB image is 24-bit, then each channel consists of 8 bits, for red, green, and blue each. Alternatively, the image is composed of three images i.e. one for each channel, where each image can accumulate discrete pixels with brightness intensities ranging from 0 to 255. Color images consist of pixels and pixels, in turn, are generated by the different combination of primary colors. Primary colors are then represented by the series of code. A **"**channel**"** is made of just one of these primary colors. Typically, RGB values are encoded as 8-bit integers, which range from 0 to 255.This is normalized to 7 bits giving 128 different values i.e.128 different values are obtained. Basically, a color hash is the graph of the number of pixels versus color variation as shown in Figure 2 and Figure 3.

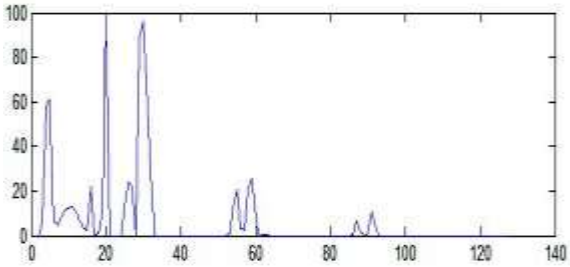

Figure 2: Graph of a Color Hash of Original Image of an Object

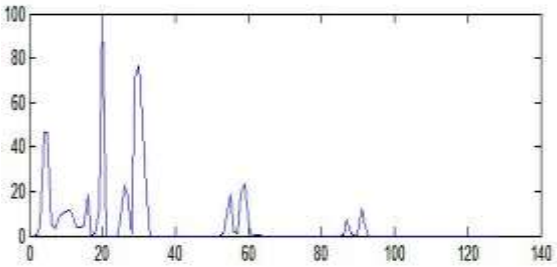

Figure 3: Graph of a Color Hash of Tampered Image of an Object

Shape Hash

In this paper, we restrict our goal to find the changes of a structure using the shape hash values. By using "shape hash" we intended to detect those regions of the object where the shape change occurred. Since last few years, histograms have been widely used to depict the images of varying size and shapes. But they fail to represent contiguous information of the image from where they were originally evaluated. There are different methods to represent shapes through histograms. To extract the feature from the image, some partial segmentation of the image is required as feature extent over the pixels only.. It is important for object recognition. It is also useful for model-based segmentation. Shape hash is the graph of the number of pixels versus the probability of edges. Edges are considered as the most basic features of the image. If the edges of an image are accurately determined, some basic properties such as shape, area, etc. can be calculated. In order to calculate the shape value, a threshold value needs to be set indicating the percentage of change in shape in case of tempering of objects. Here, a threshold value of 0.1 is set to indicate 10% of shape changes occurred.

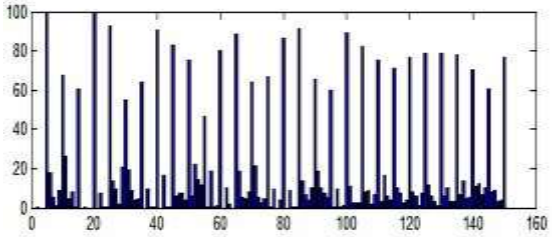

Figure 4: Graph of Shape Hash of Original Image of an Object

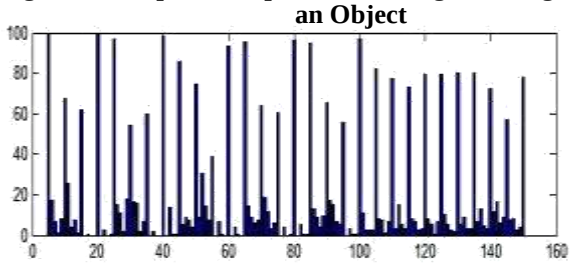

Figure 5: Graph of Shape Hash of Tampered Image of an Object

Support Vector Machine:

Support vector machines (SVM) uses supervised learning models with equivalent training algorithms which classifies the data. From a collection of training examples of images, where each image is marked as the element of one or the other of two classes, an SVM training algorithm generates a model that assigns new examples to one class or the another class, hence generating a linear classifier based on non-probabilistic theory. The data is then classified into distinct and non-distinct data.

i) Distinct Data:

Support vector machine (SVM) is predominantly used when the data mostly has two classes. The classification of data by SVM is done by finding the suitable hyper plane that distinguishes all data points of one class from those of the other class. The suitable hyper plane for an SVM corresponds to the one having the largest margin between the two classes.. The support vectors are nothing but the data points that are nearby to the separating hyper plane. These points are on the boundary of the slab.

Numerical Plan:

Let us review a supervised binary classification problem where the training data sets are denoted by $\{a_i, b_i\}$ where i=1, 2,…J , where J is the number of training samples and $b_i \in \{-1,+1\}$ where $b_i \in +1$ for class A and $b_i \in -1$ belongs to class B. Consider these two classes are linearly separable. This states that it is feasible to find at least one hyperplane defined by vector x and bias value x_0 which can separate the two classes without any errors.

$$g(x) = x^* a + x_0 \ldots (i)$$

To find a hyper plane, x and x_0 should be evaluated in such a way that:

$b_i (x^* i + x_0) \geq 1$ for $i = +1$ (for class A) and

$b_i (x^* + x_0) \leq -1$ for $i = -1$ (for class B).

ii) Non-Distinct Data

In most of the cases, it might happen that data may not permit for a separating hyper plane i.e., classes are not linearly separable. In such scenario, above equations are not suitable. For dealing with such a scenario, a penalty parameter Q and a slack variable α need to be framed. The equation is represented as

Minimize $M(x_0, \alpha) = (\|x\|^2 + Q \sum \alpha i J$

Subject to $b_i (x^* a_i + x_0) \geq 1 - \alpha i$.

Results and Conclusion

Analysis of color hash and shape hash is done with different images of the object- original as well as tampered images. Graph of the color hash of tampered image the small difference in the spike indicating that the image has tampered. Similarly the graph of shape hash show difference in spike due to change in shape of the original object. The hash vector of original image differed from the tampered image. The shape hash values varied with the change in shapes of an object. The spike found in the graph of an original image is larger than the tampered image in both color hash and shape hash. A threshold of 0.1 is set to indicate 10% of the shape changes occur during tampering. The selection of JPEG images is included in the database. The image of the object along with its features is then stored in the database. The Figure 6 shows the original images of an object stored in the database. Figure 7 shows the tampered images of the objects. Tampered status "2" represents the original image is recorded and tampered status "1" represents tampered image is recorded. The features will help in classifying the input data. The Figure 8 depicts the information about trained SVM for the analysis. The graph shown in Figure 11 shows the analysis of the image tested for the evaluating the performance.

Figure 6: Original Images of the Object

Figure 7: Tampered Images of the Object

Figure 8: Result of Trained SVM

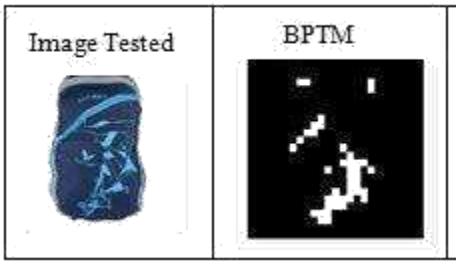

Figure 9: Binary Probability Tamper Map of the Tested Image

Figure 10: Detected Region of the Image

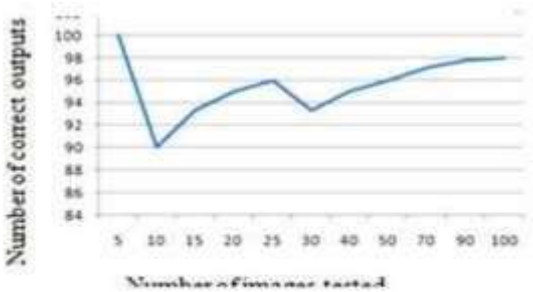

Figure 11: A Graph Showing Accuracy of the Images Tested

The scheme evaluates three aspects of object tampering detection: (1) database creation where analysis of shape hash, color hash and hash vector of the image is stored to decide whether the input image has the same content as the original one or not; (2) training of SVM is performed to record the number of inputs along with the bias value. The bias value less than 0.5 indicates more number of tampered images are recorded in the database and the bias value greater than 0.5 indicates more number of non-tampered images are recorded in a database. (3) Evaluation of SVM- classification of images are done which are stored in the database using SVM to label them as original or the tampered one which helps in the analysis of an input image. This localizes the region of tampering in the image of the object using the tamper map. The proposed approach can be used to detect any modification in the object content. Results show that the color hash and the shape hash is used to indicate or find the changes occurred in the image of the object. Also, here accuracy is evaluated in terms of number of images tested versus number of correct outputs of the tested images. In our future work, we will investigate how geometrical transformation affects the tempering detection of objects. In this paper, we presented an approach of using color hash and shape hash to detect any modification in the structure of an object. The modified values of the color hash and shape hash indicated a change in color texture and shape of the object respectively. The alteration in the structure of an object can, however, can be shown with histograms but using color hash and shape hash gave better accuracy than histograms. In Figure 9, the Binary Probability Tamper Map shows the regions of abrupt change in the structure of object after tampering. The region coloured in white shows the more concentrated area of tampering found in the image. The region coloured in black shows less concentrated regions of tampering. This method helps us to localize the region of tampering in object. Figure 10 shows the detected regions of image.

References

1. Pun Chi-Man, Yan Caiping, and Yuan Xiao-Chen, 2017, Image Alignment-Based Multi-Region Matching for Object-Level Tampering Detection, IEEE Transactions On Information Forensics And Security, Vol. 12, No.2, 377.

2 Venkatesan R, Koon S. M, Jakubowski M. H., and Moulin P., 2000, Robust image hashing, Proc. Int. Conf. Image Process., vol. 3, 664–666.

3. Monga V., Vats D, and Evans B. L., 2005, Image authentication under geometric attacks via structure matching, Proc. IEEE Int. Conf. Multimedia Expo (ICME), 229–232.

4. Wang X., Pang K., Zhou X., Zhou Y, Li L., and. Xue J, 2015, A visual model-based perceptual image hash for content authentication, IEEE Trans. Inf. Forensics Security, vol. 10, 7,1336–1349,

5. Yan C.-P, Pun C.-M, and. Yuan X.-C, 2016, Multi-scale image hashing using adaptive local feature extraction for robust tampering detection, Signal Process., vol. 121, 1–16.

6. Irani M.and Anandan P., 1999, About direct methods, Proc. Int. Workshop Vision Algorithms, ICCV, Corfu, Greece, 267–277.

7. Torr P. H. S and Zisserman A., 1999, Feature-based methods for structure and motion estimation, Proc. Int. Workshop Vision Algorithms, Corfu, Greece, 278–294.

8. Szeliski R., 2006, Image alignment and stitching: A tutorial, Foundations Trends Computer Graphics Computer Vision, vol. 2, 1, 1–104

9. Lu W, Varna A. L., and. Wu M, 2010, Forensic hash for multimedia information,

Proc. SPIE Electronic Imaging Symp.—Media Forensics Security.
10. Lu W and Wu M, 2010, Multimedia forensic hash based on visual words, Proc. IEEE Computer Soc. Int. Conf. Image Processing, 989–992.
11. N.N.Khalsa, Parag.P.Gudadhe, Dr. V. T. Ingole, 2014, Advanced Image Classification System, International Journal of Computer Science and Information Technologies, Vol. 5, 3210 – 3214
12. Khalsa Nikko. IngoleDr. Vijay T, 2014, Novel method for classification of Artificial and Natural images, International Journal Of Scientific & Engineering Research, France Volume 5, Issue 3.
13. Gudadhe Parag, Khalsa Nikko, 2014, Features affecting the classification of images, International Journal of Recent Development in Engineering and Technology, Volume 2, Issue 3.

