Tamper Detection in Image using Voting Procedure Algorithm

Ms Swaleha Chougale*, Mrs. Anis Mulla, Mr.Sandeep Sutar****

* Department of CSE, ADCET, Ashta
** Department of CSE, ADCET, Ashta
*** Department of CSE, ADCET, Ashta

Abstract- In today's world seeing is no longer believing- the technology that allows for digital visual data to be manipulated is developing at great speed. The quick advance in image editing techniques has enabled people to synthesize realistic images conveniently. Some legal issues may arise when a tampered image cannot be distinguished from original one by visual examination. In this paper Scale Invariant Feature Transform algorithm is used to extract interest points of an image. Voting procedure algorithm is used to determine transformation with respect to X-axis and Y-axis. Final results differentiates tampered image from original image

Index Terms- Image Processing, Scale Invariant Feature Transform, Tamper Detection, Voting Procedure Algorithm.

I. INTRODUCTION

An image is "tampered" means part of the content of a real image is altered. An image is tampered implies that it must contain two parts: 1) Unchanged region 2) Tampered region. Due to the ease of generating and modifying images it is critical to establish trust worthiness for online multimedia information. The assessment of the reliability of an image received through the Internet is an important issue. Images are widespread on today's internet and cause significant social impact, which can be evidenced by the increase of social networking sites with user generated contents. Specifically, methods useful to establish the validity and authenticity of a received image are needed in the context of Internet communications. It uses signature-based approaches. In this, the image hash is associated with the image as header information and must be small and robust against different operations.

In order to perform tampering localization, the receiver should be able to filter out all the geometric transformations (e.g., rotation, scaling) added to the tampered image, in order to align the received image with the one at the sender. An image hash is a distinctive signature which represents the visual content of the image in a compact way (usually just few bytes). The image hash should be robust against allowed operations and at the same time it should differ from the one computed on a different/tampered image. Image hashing techniques are considered extremely useful to validate the authenticity of an image received through a communication channel.

II. SIGNIFICANCE

The quick advance in image editing techniques has enabled people to synthesize realistic images conveniently. Some legal issues may arise when a tampered image cannot be distinguished from a real one by visual examination. This approach outperforms recently appeared techniques by obtaining a significant margin in terms of registration accuracy and tampering detection. Methods generate encouraging results to improve the accuracy of tampering detection using in depth analysis.

It needs to perform more in depth analysis to establish the minimal number of scale invariant feature transform needed to guarantee an accurate estimation of the geometric transformations. Comparative tests shows that the approach outperforms recently appeared techniques, it better deal with texturized and contrasted tampering patches.

III. TAMPER DETECTION IN IMAGE

As shown in figure 1, our system is useful in Tamper Detection in Images. This system generally divides into six parts. It first takes an image as an input. Then we applied Scale Invariant Feature Transform (SIFT) algorithm to extract interest points of an image. Extracted interest points are stored in XML file format. Interest points are represented using descriptor of size 128 dimension. For Codebook generation purpose we have suggested a K-means clustering algorithm. Codebook is generated by using interest points of database images. Codebook uses SIFT descriptors and obtains values in the form of Centroid_X and Centroid_Y. Matching of interest points of original image and input image is performed. To match the interest points of input image against interest point's database images, Nearest Neighbor method is used.

Matched interest points are used as an input in Voting Procedure algorithm. It finds transformation with X-axis (Tx), Y-axis (Ty) and Rotation angle α. The values of Tx, Ty and α are used for Image Alignment. Image has been registered before Tamper detection. The proposed technique is utilized to differentiate between original image and Tampered image.

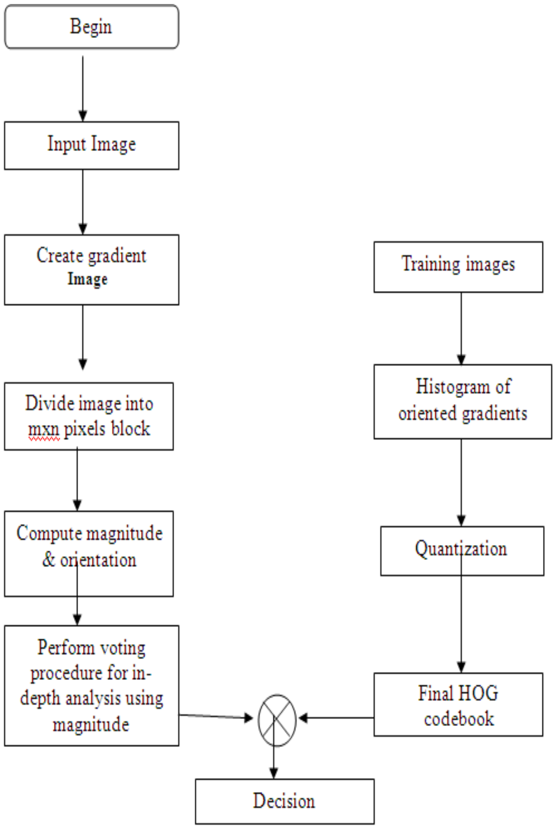

Begin
Input Image
Create gradient Image
Divide image into mxn pixels block
Compute magnitude & orientation
Perform voting procedure for in-depth analysis using magnitude
Training images
Histogram of oriented gradients
Quantization
Final HOG codebook
Decision

Figure 1: System work flow

System is categorized into following parts:

A) Extraction of Interest Points:

Following steps generates interest points of input image:

1) Construct Scale Space:-

Gaussian Kernel is used to create scale space.

$$L(x, y, \sigma) = G(x, y, \sigma)* I(x, y)$$

2) Take Difference of Gaussian(DoG):-

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma))* I(x, y)$$
$$= L(x, y, k\sigma) - L(x, y, \sigma)$$

3) Locate DoG Extrema:-

Scan each DoG image. Look at all neighboring points. Identify min & max by making 26 comparisons. Large number of Extrema computationally expensive. So detect most stable subset.

4) Sub Pixel Localization:-

It uses Taylor series expansion to get location in terms of x, y, and σ.

5) Filter Edge & Low Contrast Responses:

It uses Hessian metrics to calculate Trace & Determinant.

6) Build Keypoint Descriptors:

Size of descriptor is128 Dimension

B) Code book Generation:

By applying K-means clustering on interest points, generate different clusters of database images & get their centroids. The codebook is generated by using different parameters of centroids of clusters. This codebook with visual words has been employed to compare the different approaches. The codebook has been learned from overall SIFT descriptors extracted on training images.

C) Matching Interest Points of Original & Tampered image:

The key points against database obtained from training images can be matched with input images. Find the nearest neighbor i.e. a keypoint with minimum Euclidean distance. It uses ratio of distance between best match & second best match.
1) If this ratio is low, then keep it.
2) If this ratio is 0.8, then discard the match.

This model, deals with matching interest points of both original & tampered image. Matching of interest point will be based on matching of their descriptors which are employed by Extraction of Interest points. Result of this will be matching pair's f key points (x_s y_s and x_r y_r) in both original image & tampered image.

D) Implementation of Voting Algorithm:

It uses x_s y_s and x_r y_r pairs obtained in Matching Interest Points in Original Image and Tampered Image. It computes transformation with X-axis (T_x) and transformation with Y-axis (Ty). T_x and T_y are computed using following formulae:

$$T_x = ((x_s\cos\alpha – y_s\sin\alpha) / (x_s\sin\alpha + y_s\cos\alpha)) (Ty-y_r) + x_r$$

$$T_y = ((x_s\sin\alpha + y_s \cos\alpha) / (x_s\cos\alpha - y_s\sin\alpha)) (Tx-x_r) + y_r$$

Rotation angle α will be computed by using Tx and Ty.

E) Image alignment & Image Registration:

The aim of the alignment phase is the estimation of the quadruple Scaling, Rotation, X-Transformation, Y-Transformation. In the process of image alignment, transform image to original position as of source image using transformation Tx, Ty and rotation angle of Bins.

For image registration the image is usually divided into non-overlapping blocks which are represented through feature vectors computed using their content.

F) Tampering Detection:

Image tampering detection will start after successful registration. The comparison of histograms of corresponding blocks is usually performed through a similarity measure (e.g., Euclidean distance, minimum intersection, etc.) and a thresholding procedure.

This procedure we will find Euclidean distance between different blocks of image and then comparison of the signatures will perform block-wise.

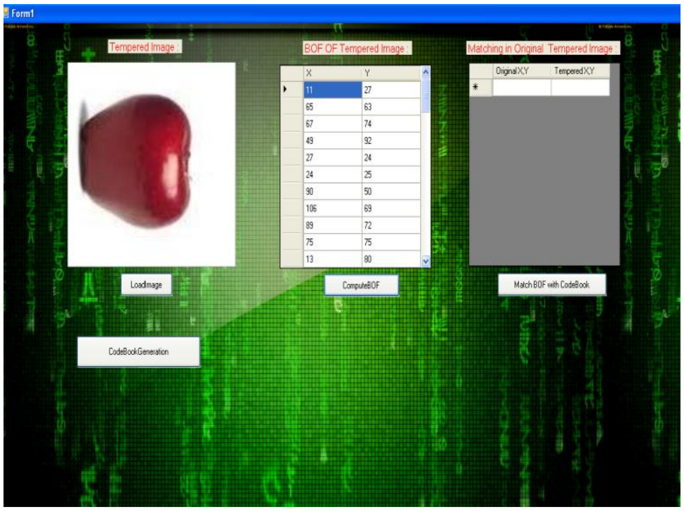
On the basis of Euclidean distance of represented blocks of tampered and not tampered image regions, tampered blocks can be highlighted.

IV. EXPERIMENTAL SETUP

In proposed system, we initially tried an implementation of Extraction of Interest points. For which it takes the input image and then by using Scale Invariant Feature transform algorithm it extracts the interest points of an input image. It represents result in the form of X-location and Y-location of interest points.

In Codebook generation, interest points of database images are extracted. K-means clustering algorithm is applied on extracted interest points to generate Codebook. It represents the result in the form of Centroid of X values (Centroid_X) and Centroid of Y values (Centroid_Y).

V. EXPERIMENTAL RESULT



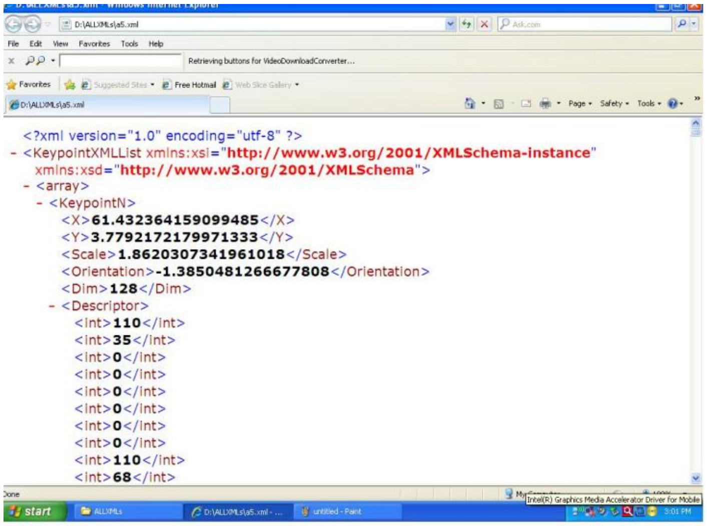
X	Y
11	27
65	63
67	74
49	92
27	24
24	25
90	50
106	69
89	72
75	75
13	80

Original X,Y	Tempered X,Y

Figure 2: Extraction of Interest Points

.

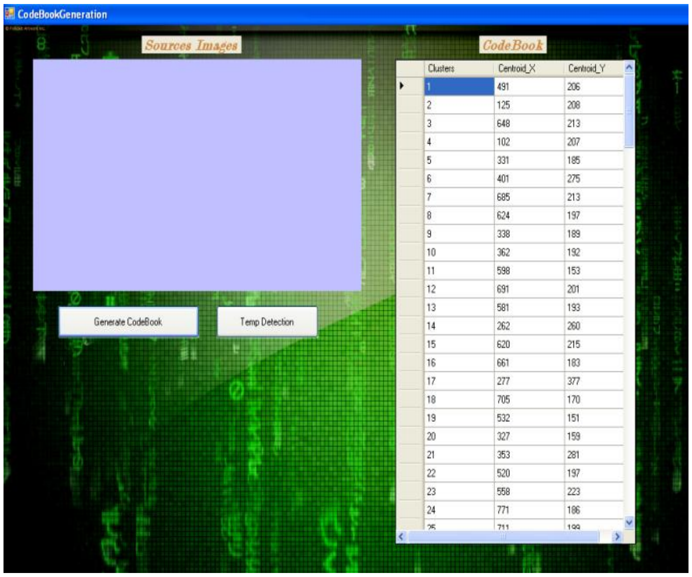
Figure 2 shows extracted interest points of input image with respect to X and Y-location.



```
  <?xml version="1.0" encoding="utf-8" ?>
- <KeypointXMLList xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  - <array>
    - <KeypointN>
        <X>61.432364159099485</X>
        <Y>3.7792172179971333</Y>
        <Scale>1.8620307341961018</Scale>
        <Orientation>-1.3850481266677808</Orientation>
        <Dim>128</Dim>
      - <Descriptor>
          <int>110</int>
          <int>35</int>
          <int>0</int>
          <int>0</int>
          <int>0</int>
          <int>0</int>
          <int>0</int>
          <int>0</int>
          <int>110</int>
          <int>68</int>
```

Figure 3: a1.xml file

Figure 3 shows Xml file format used for storing interest points. Interest point descriptor is of size 128 dimension.



Clusters	Centroid_X	Centroid_Y
1	491	206
2	125	208
3	648	213
4	102	207
5	331	185
6	401	275
7	685	213
8	624	197
9	338	189
10	362	192
11	598	153
12	691	201
13	581	193
14	262	260
15	620	215
16	661	183
17	277	377
18	705	170
19	532	151
20	327	159
21	353	281
22	520	197
23	558	223
24	771	186
25	711	199

Figure 4: Codebook Generation

Figure 4 shows Codebook of database images. It is generated by using K-means clustering algorithm. Results obtained from Codebook generation are used for matching interest points of original image and input image.

VI. CONCLUSION

First literature survey is carried out on image processing techniques. Then we identified the need to extract key features of an image and we proposed "Tamper Detection in Image using Voting Procedure Algorithm". We have implemented Extraction of interest points of input image and Generation of Codebook of dataset.

Our future work will attempt to implement the remaining system.

REFERENCES

[1] Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, and Giovanni, "Robust image alignment for tampering detection," *IEEE Transactions on Information Forensics and Security, Vol. 7, no. 4, August* 2012.

[2] D. G. Lowe, "Distinctive image features from scale-invariant key points," *Int. J. Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[3] S. Lazebnik, C. Schmid, and J. Ponce, "Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories," in *Proc. IEEE Computer Soc. Conf. Computer Vision Pattern Recognition*, 2006, pp. 2169–2178.

[4] M. Brown, R. Szeliski, and S. Winder, "Multi-image matching using multi-scale oriented patches," in *Proc. IEEE Conf. Computer Vision Pattern Recognition*, 2005, vol. 1, pp. 510–517.

[5] S. Battiato, G.M. Farinella, E.Messina, and G. Puglisi, "Robust image registration and tampering localization exploiting bag of features based forensic signature," in *Proc. ACM Multimedia (MM'11),* 2011.

[6] Online Available: http://www.google.co.in/

[7] A.K.Jain,"Fundamentals of Digital image processing", a book.

AUTHORS

First Author – Ms.Swaleha Chougale, ME (CSE)App, ADCET,Ashta,swalehachougale09@gmail.com.
Second Author – Mrs. Anis Mulla, MTECH(CSE), ADCET,Ashta,mulla.anis@gmail.com.
Third Author – Mr.Sandeep Sutar, ME(CSE), ADCET,Ashta,sutarsandeep@gmail.com.