Manipulated Image Detection by using Scale Invariant Feature Detection Algorithm

Swaleha B.Chougale
Annasaheb Dange College of Engineering and Technology, Ashta, Tal-Walwa Dist-Sangli.

Anis Mulla
Annasaheb Dange College of Engineering and Technology, Ashta, Tal-Walwa Dist-Sangli.

Dhanashee V Patil
Annasaheb Dange College of Engineering and Technology, Ashta, Tal-Walwa Dist-Sangli.

ABSTRACT
We deal with large amount of multimedia data either audio, video or image. 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 manipulated 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 manipulated image from original image.

General Terms
Scale Invariant Feature Transform, Manipulation Detection, Voting Procedure Algorithm

Keywords
Image, image editing techniques.

1. INTRODUCTION
An image is "Manipulated" means part of the content of a real image is altered. An image is manipulated implies that it must contain two parts: 1) Unchanged region 2) Manipulated region. Several image editing techniques are available. 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 manipulated part localization, the receiver should be able to filter out all the geometric transformations (e.g., rotation, scaling) added to the manipulated 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 manipulated image. Image hashing techniques are considered extremely useful to validate the authenticity of an image received through a communication channel.

2. LITERATURE SURVEY
a) Authors Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, and Giovanni [1] have suggested Codebook Generation. A codebook is generated by clustering the set of SIFT extracted on training images. The clustering procedure points out a centroid for each cluster. The set of centroids represents the codebook to be used during the image hash generation. The computed codebook is shared between sender and receiver. Codebook is built only once, and then used for all the communications between sender and receiver. The tampering manipulation typically changes the properties (e.g., edges distributions, colors, textures, etc.) of some image regions. To deal with this problem the image is usually divided into non-overlapping blocks which are represented through feature vectors computed taking into account their content. The feature vectors computed at the source are then sent to a destination where these are used as forensic hash for the tampering detection component of the system. The check to localize tampered blocks is performed by the receiver taking into account the received signature and the one computed (with the same procedure employed by the sender) on the received image.

b) Authors S. Battiato, G.M. Farinella, E.Messina, and G. Puglis [2] have specified techniques for image registration and tampering localization. Tamper Detection in Images using Voting Procedure Algorithm. It deals with recovering geometric transformations occurred on a received image from its signature. A codebook is generated by clustering the set of SIFT (scale invariant feature transform) extracted on training images. Codebook is built only once, and then used for all communication between sender and receiver. A more effective way to deal with the problem of wrong matching has been used, where strategy based on the scale-invariant feature transform (SIFT) dominant directions combined in cascade with a robust estimator based on a voting strategy on the parameter space is presented.

3.3: Understanding geometric manipulations of images through BOVW-based Hashing

c) Authors S. Battiato, G.M. Farinella, E.Messina, and G. Puglis [3] Describes concept of Image hash. It 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 the Internet .A more robust approach based on a cascade of estimators has been introduced; it is able to better handle the replicated matching in order to make a more robust estimation of the orientation parameter.

Moreover, the cascade of estimators allows a higher precision in estimating the scale factor.

d) Authors S. Roy and Q. Sun [4] have provided image hashing method consists of two steps: (1) Hash generation (2) Verification. Image hashing methods (that primarily address the issue of robustness) can be categorized as belonging to (a) Exhaustive search based approach. (b) Robust representation based approach. Exhaustive search based methods clearly suffer from impractical levels of search complexity, Lack of content information as part of the hash also leads to high false positive detection error. The problem of localizing tampering in images can also be solved using a watermarking based approach, wherein, a watermark is inserted into the image at the point of creation, and during verification, the watermark is extracted to verify if there was any allowable modification or illegal manipulation performed on the image. Any tampering can be localized from the damage to the watermark.

3. COMMENTS

From the above survey we can comment that,

- 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
- Method produces encouraging results to improve the accuracy of tampering detection using in depth analysis.

4. NEED OF WORK

Hash encodes the spatial distribution of features to better deal with highly texturized and contrasted tampering patches. 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.

5. PROPOSED WORK

The orientation histograms related to blocks extracted on training images are clustered taking into account their similarity (Euclidean distance). The prototypes (i.e., centroids) of the produced clusters are retained to form the vocabulary. Images at sender and receiver are first split into blocks and then each block is associated to the closest histogram prototype belonging to the shared vocabulary. Comparison between signatures is made by simply comparing the IDs of corresponding blocks after the alignment.

5.1.4 Voting Procedure 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:

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

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

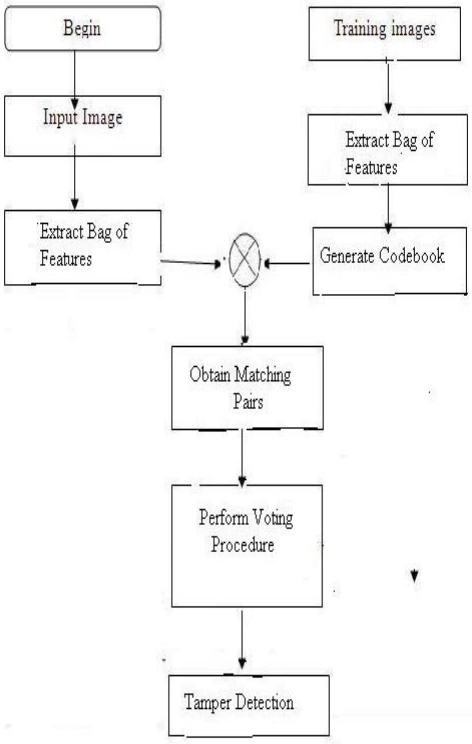

Figure 1: System Architecture

Figure 1 shows architecture of proposed system, in which k-means clustering algorithm is used to generate Codebook. Extracted features of input image are compared with Codebook. Result of this comparison is matching pairs of input image & original image

5.1 The Modules of the Proposed Work

5.1.1 Extraction of Bag of Features:

It uses Scale Invariant Feature Transform (SIFT) algorithm to extract features of Input Image. To increase accuracy in obtaining features, it takes blurred image. Extracted features are stored in xml file format

5.1.2 Generate Codebook:

In this module, features of training images are extracted. On extracted points k-means clustering algorithm is applied. Obtained results are stored in xml file format

5.1.3 Matching of Bag of Features of Original Image and Manipulated Image:

In this module extracted interest points of input image are compared with the codebook. Result obtained from this module is used as input for Voting Procedure Algorithm.

5.1.5 Manipulation 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.

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

6. EXPERIMENTAL SETUP AND RESULTS

In this system, we extracted interest points of training images. On interest points K-means clustering algorithm is applied. It generates result in the form of Codebook.

Also Extracted interest points of input image. Extracted interest points are compared with Codebook. It Produces matching pairs. Matching pairs are used as an input for Voting Procedure Algorithm

6.1 Results

Here, we have shown the result of work.

Figure 2 : Extraction of Interest Points

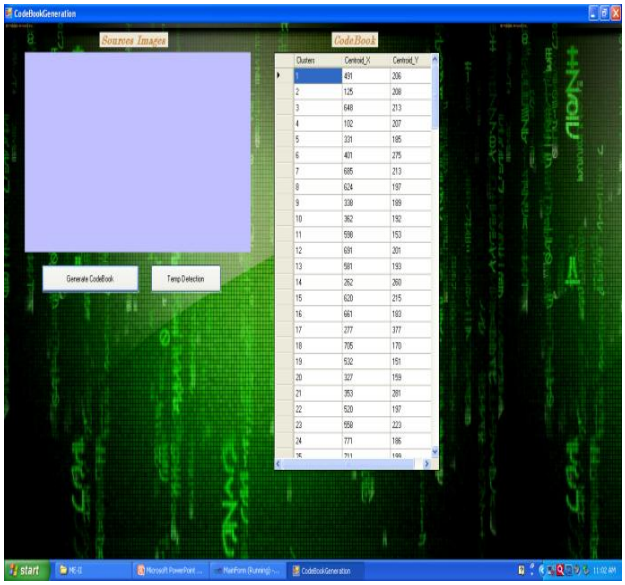

Figure 3: Codebook Generation

Figure 3 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.

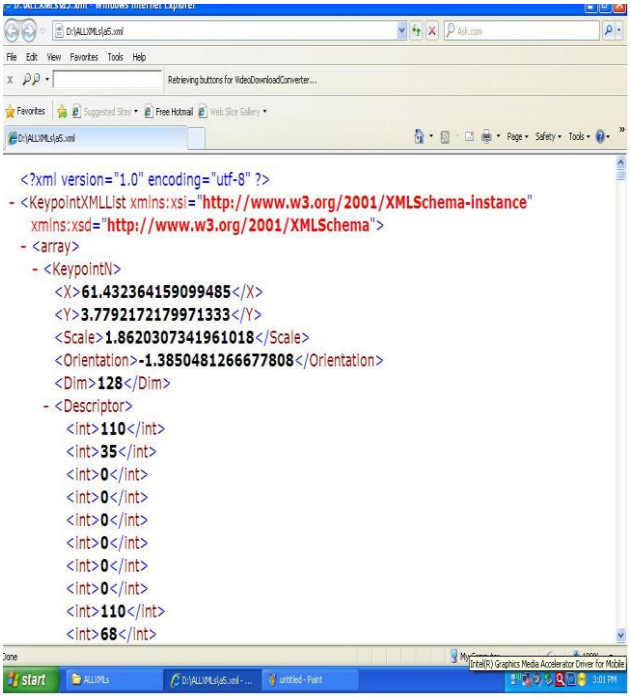

Figure 4: a1.xml file

Figure 4 shows Xml file format used for storing interest points. Interest point descriptor is of size 128 dimension.

Figure 5: Matching Interest Points

It shows the result of Matching of Interest points of input image & original image.

Figure 6: Manipulation Detection

It shows the region of an image where manipulation has been occurred.

7. 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 "Manipulated Image Detection using Scale Invariant Feature Transform Algorithm." It works for JPEG image format

Our future work will attempt to implement the system that will support all image formats.

8. ACKNOWLEDGEMENT

I would like to thanks my guide Prof.A.N.Mulla for her valuable and constructive comments. I would also like to thanks Dr Nitin Trivedi, HOD Computer Science & Engineering Department, Annasaheb Dange College of Engineering & Technology, and Ashta for his valuable support.

9. 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.