# Authentication and Tampering Detection of Transferred Image

Swati Shivaji Bhosale, Research Scholar
Department of Computer Engineering,
Vidya Pratishthan College of Engineering, Baramati,413 133, University of Pune, Maharashtra, India.

Gyankamal J. Chhajed, Assistant Professor,
Department of Computer Engineering,
Vidya Pratishthan College of Engineering, Baramati,413 133,
University of Pune, Maharashtra, India.

***Abstract* — In today's era, technology is developing at great speed. There are many ways available to manipulate digital visual content. This leads people to edit images conveniently and quickly. When the image cannot be distinguished only by visual examination, some legal issues may arise. The image that is sent at the destination over the network should be the same as at the source side. But it is very difficult to trust on the received contents without any check, especially in the areas where the source image is unknown and one has to use data that is available about the image only. In this context, the problem of authentication of received image is handled. In this paper authentication and tampering detection of transmitted image is proposed with the use of scale invariant feature transform algorithm to extract the interest point of the image. These points are used to create signature, which further is transmitted along with image and analyzed at the destination for authentication. The voting procedure is performed to determine transformations such as rotation, scale and to align the received image. In this method image is divided into blocks and for the tamper detection comparison of histograms of gradients is used.**

***Keywords— Image authentication, tampering detection, Scale Invariant Feature Transform (SIFT), Histogram of Gradients***

## I. INTRODUCTION

The increasing techniques in image editing and to protect the digital visual data against malicious manipulations makes the use of visual content as evidence material unreliable. It puts question on trust worthiness of digital online multimedia information. Therefore the techniques that are used for validity and authenticity of a received image are needed in context of internet communication.

The image authentication process checks the image for its originality. Tampering of image means the part of the real image is altered. Thus the image has two areas, tampered area and unchanged area. In order to perform tampering localization all geometric transformation (e.g. rotation, scaling etc.) should be first filtered out, so that alignment of received image can be done as with the one at the sender. The signature of image implies all the important data related to the image key points which are used for the authentication of received image at destination. The signature of image signature should be much compact, robust against the allowed operations and also it should differ from the one that is computed on tampered image.

The tampering detection is the process of finding out tampered areas in image which is based on block wise searching. Image is divided into blocks and with the histograms of gradients representation, the tampering detection and localization is done. The overall process takes following steps:

1. *Feature Extraction*: The features of image dataset are extracted and a vocabulary of features is formed, and then it is shared to sender and receiver. At source the features of image that is to be sent are calculated, signature with most robust features is prepared and it is sent with image itself to the destination.
2. *Signature Comparison*: At destination same procedure is applied for received image to get signature. The both signatures are compared and similarities are found out. With help of similar features data the image alignment is done.
3. *Tampering detection*: The received image is divided into blocks and HoG for each block is prepared. These histograms are compared with the received histogram data and the tampered area is found.

Section II briefly describes the different methods available in this context. Section III gives implementation details of proposed approach to get tampering detection. Section IV gives the details about dataset used for this system and the result analysis. At last, we conclude this paper with future work.

## II. LITERATURE SURVEY

In today's technology habitual world, the demand of techniques useful to protect digital visual data against malicious manipulations is increasing rapidly. The techniques used for image editing are putting questions on use of the visual content as evidence material [10]. For this reason, methods useful to establish the validity and authenticity of a received image are needed. Various methods can be used for tampering detection such as Watermarking based approach, use of signature techniques.

In the watermarking methods the watermark is added into the image and it is extracted for verification of malicious manipulation on the received image, in the tampering detection process. Damage into the watermark shows a tampering of the image under consideration. A disadvantage in using watermarking method is the need for distorting the content. Digital watermarking algorithms are composed of three parts, namely, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm.

The signature based approach has been introduced to overcome above problem. In this method the image signature is not inserted into the image; rather it is used in association with the image as header information. It must be compact and robust against different operations. Different signature-based approaches have been proposed in literature [2], [4], and [6]. These approaches use the same basic scheme as:

- Image is sent with the signature code attached to it.
- This signature is analyzed at destination for the reliability of the received image.

Image hashing techniques are considered very useful to validate the authenticity of an image received through the communication.

The approach in [3], [4] states that the hash which represent the visual content of image should be compact and robust. It should differ from the hash of tampered or different image. In many applications the source image is not known. In such cases the hash states all the information about the image.

The different alignment techniques that are proposed [7], [1] are unsuitable forensic hashing since the basic requirement is that for the reduction in network communication the signature should be compact.

The estimation of geometric parameters (rotation, scale etc.) is proposed in [9] whereas image hash based on invariant features of image is proposed in [4]. [5] uses bag of features model to represent features that are used in image hash.

In previous works [2], [4], and [5] only contrast properties were considered for feature selection which is not robust against malicious attacks. Considering contrast properties and spatial distribution of the features, the selection method is proposed. To get the features of image, Scale Invariant Feature transform [9] is used.

## III. BASIC TERMINOLOGY

The Proposed system called Authentication and Tampering detection of transferred image with its alignment using SIFT and HoG address the problem of image alignment, authentication and tampering detection. For a given user image file, the proposed method interacts with the image features to use in alignment of received image which is further used for tampering detection. Proposed System is able to detect the tampered areas in the image.

It uses the SIFT algorithm for extracting the image features and the histogram representation of image blocks to get the tampered areas. The features of different images are extracted and a codebook is generated which is shared between the sender and receiver. Also the histogram of gradients codebook is generated and shared. Sender sends the image and the hash of the image features. Receiver also calculates hash with same method and authenticates and aligns the received image. Then the received image is divided into blocks and histograms of blocks are calculated. These histograms are compared with previously generated histograms codebook and the tampered area in image is found out.

The system architecture is as shown in Fig. 1.

The proposed system is divided into four blocks.

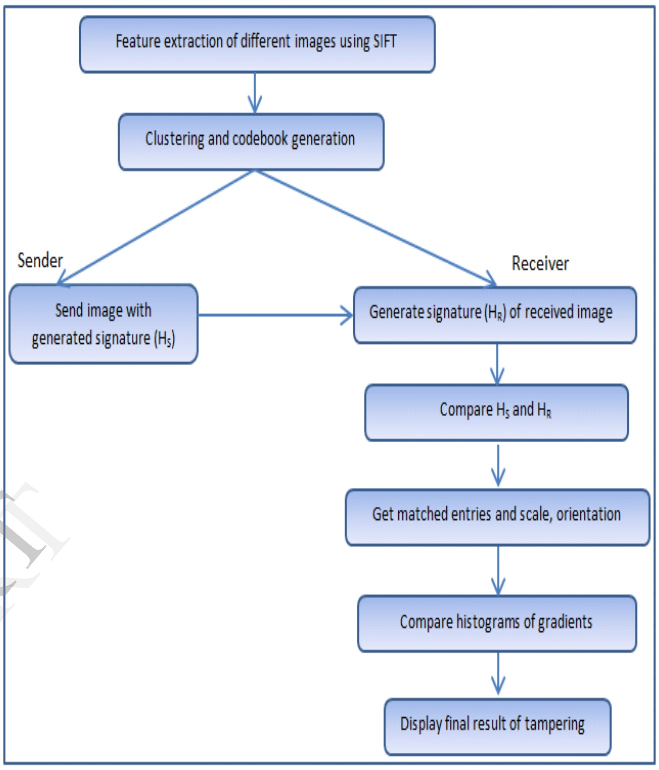

Feature extraction of different images using SIFT
Clustering and codebook generation
Sender
Receiver
Send image with generated signature ($H_S$)
Generate signature ($H_R$) of received image
Compare $H_S$ and $H_R$
Get matched entries and scale, orientation
Compare histograms of gradients
Display final result of tampering

Fig.1. System Architecture

1. Codebook and histograms of gradients representation: The features of the collected images are extracted using the Scale Invariant Feature Transform algorithm. These are the points on the image. The top n features are selected for the further process which will be the robust, that we can get them though the image undergoes any allowed changes. These features are clustered using k-means algorithm to get centroids which represents the codebook. To calculate the histograms of gradients the image is divided into non overlapping blocks of n x n size.

The contents of each block are feature vectors which are represented by the gradient histograms. These blocks are clustered considering their similarities. The vocabulary is formed producing their centroids. These histograms are sent to the receiver and the codebook is shared with sender and receiver. Codebook is generated and shared only once to reduce network communication.

2. Prepare the Image Signature: Sender extracts the features of image that is to be sent and sorts them according to their contrast values in descending order. The top n SIFT are selected and the id label is assigned to them with help of codebook. The signature will contain the id label, the

coordinates (x, y) and the direction. The image and the hash are sent to the destination. The signature is sent through the trusted network whereas image is sent via untrusted network. Receiver creates the signature of received image using the same method employed by the sender. Then considering the id labels, the entries of the signatures are matched.

3. Image registration: The matched entries are used for alignment of received image which uses rotation angle and the scaling factor. It is assumed that the point ($x_r$, $y_r$) in destination image is a transformation of the point ($x_s$, $y_s$) in the source image, with the combination of translation ($T_x$,$T_y$), rotation(α), and scaling(α). This alignment phase aims at the estimation of the ($T_x$, $T_y$, α, σ) quadruple by corresponding the matches (xs, ys) of source signature, and the ($x_r$, $y_r$) of destination signature.

Similarity transformation of key point pairs corresponding to matched signatures entries is employed:

a. $x_r = x_s\sigma \cos\alpha - y_s\sigma \sin\alpha + T_x$

b. $y_r = x_s\sigma \sin\alpha + y_s\sigma \cos\alpha + T_y$

To calculate the parameters, we consider the differences between dominant directions of the signature entries with corresponding id,

$$\theta = \theta_{r,i} - \theta_{s,j} \mid id_{s,i} = id_{r,j} \; ; i = 1,\ldots\ldots,n \qquad \text{------(1)}$$

and the ratio of scales of the matching between hs and hr,

$$\Sigma = \{ (\sigma_{r,i} \;/\; \sigma_{s,j}) \mid id_{r,j} \; ; i, j = 1,\ldots\ldots,n\} \qquad \text{------(2)}$$

The system design for authentication and alignment is shown in Fig. 2.

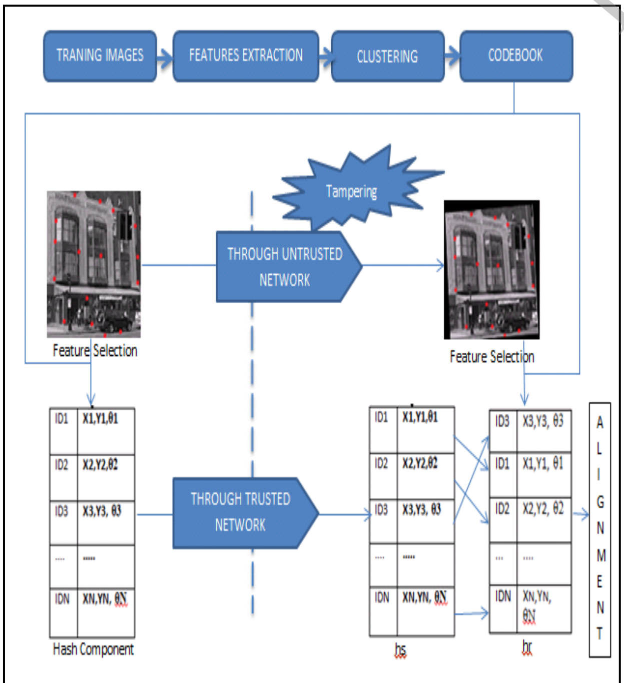


Fig. 2 Codebook & signature Preparation

4. Tampering Detection: After the alignment of image, the examination of image for detection of tampered regions is prepared. Tampering localization is the process of finding out the regions of the image that have been deployed for malicious purpose to change the meaning of the visual message. Typically the tampering in the image changes the properties (e.g. edges, colors, textures etc.) of some regions of the image. The tampering in the image is detected by dividing the image into non-overlapping blocks, these blocks represent the feature vectors. The histograms of gradients representation is used to describe the contents of each block. For each block of image HoG are generated. These histograms are then compared through the similarity measure (e.g. Euclidean distance etc.) with the data that the receiver received already. The receiver adopts a method to compare both the histograms and generates the result.

The tampering detection system design is as in Fig. 3.

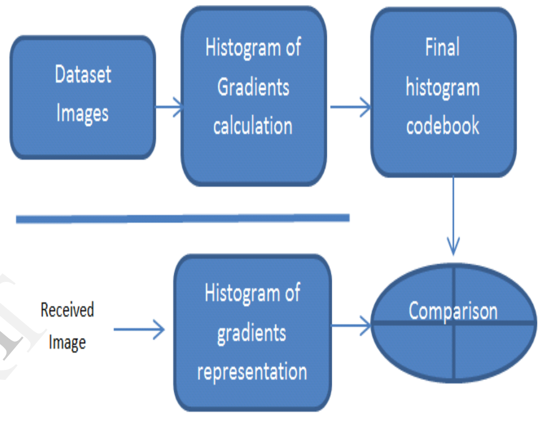

Dataset Images
Histogram of Gradients calculation
Final histogram codebook
Received Image
Histogram of gradients representation
Comparison

Fig.3 Tampering Localization at receiver

The following table shows the operations with parameters that are allowed as image transformations in the system.

Table- I
Image Transformations

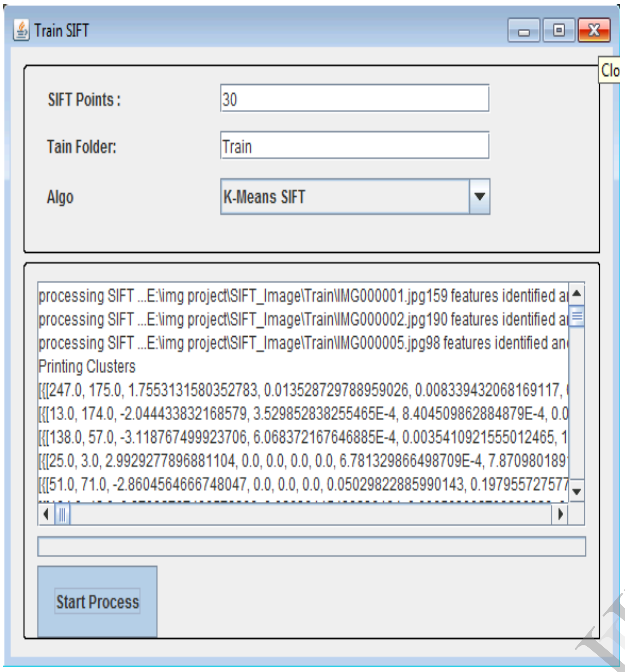
| Operation | Parameter |
|---|---|
| Scaling (σ) | 0.5, 0.7 |
| Rotation (α) | 3, 5 degrees |
| Horizontal translation (Tx) | 5, 10 pixels |
| Vertical Translation (Ty) | 5,10 pixels |

## IV. RESULT ANALYSIS

The system uses an image dataset in which images are taken from different categories such as kitchen, industrial, forest etc. The features extracted through SIFT are stored for clustering purpose. The use of images in different areas allows coping with variability needed in context of image authentication and tampering. The image transformations as rotation, translation, scaling are considered here which are available on any manipulation software.

As the Scale Invariant Feature Transform is used, we get the robust features of image. The sharing of codebook and histogram of gradients reduces the network communication.

The following images are the screenshots of the implemented system. Screenshot-1 shows the values in the clusters. Screenshot-2 shows the tampering detection percentage and the matched image from training set for selected test image. The Graph-1 shows is the analysis for number of matched images in the test set with the training set images for given amount of signature values.



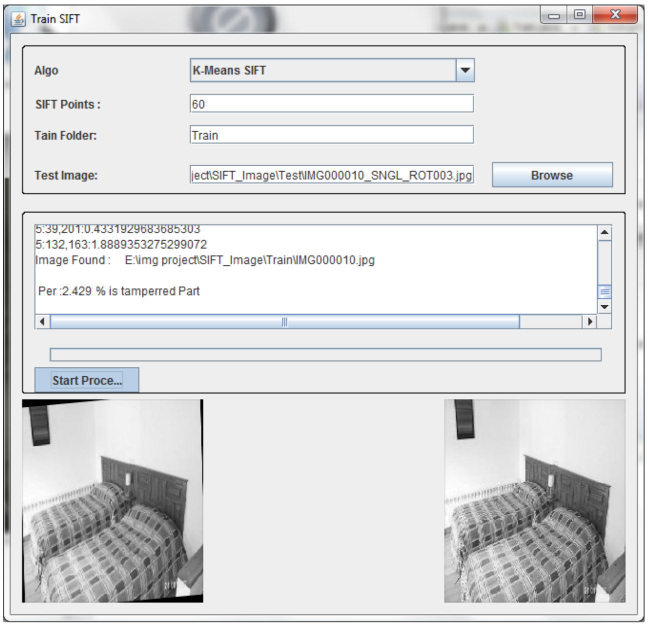
SIFT Points : 30

Tain Folder: Train

Algo K-Means SIFT

```
processing SIFT ...E:\img project\SIFT_Image\Train\IMG000001.jpg159 features identified a
processing SIFT ...E:\img project\SIFT_Image\Train\IMG000002.jpg190 features identified a
processing SIFT ...E:\img project\SIFT_Image\Train\IMG000005.jpg98 features identified an
Printing Clusters
[{[247.0, 175.0, 1.7553131580352783, 0.013528729788959026, 0.008339432068169117,
[{[13.0, 174.0, -2.044433832168579, 3.529852838255465E-4, 8.404509862884879E-4, 0.0
[{[138.0, 57.0, -3.118767499923706, 6.068372167646885E-4, 0.003541092155501246 5, 1
[{[25.0, 3.0, 2.9929277896881104, 0.0, 0.0, 0.0, 0.0, 6.781329866498709E-4, 7.870980189
[{[51.0, 71.0, -2.860456466674804 7, 0.0, 0.0, 0.0, 0.05029822885990143, 0.19795572757
```

Screenshot 1: Printing cluster data



Algo K-Means SIFT

SIFT Points : 60

Tain Folder: Train

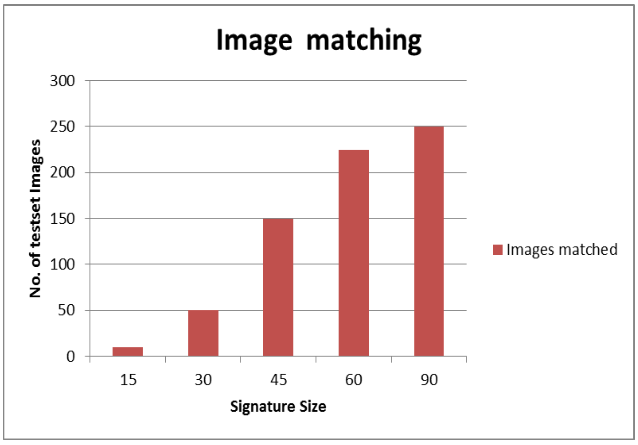
Test Image: ject\SIFT_Image\Test\IMG000010_SNGL_ROT003.jpg

```
5:39,201:0.4331929683685303
5:132,163:1.8889353275299072
Image Found :    E:\img project\SIFT_Image\Train\IMG000010.jpg

 Per :2.429 % is tamperred Part
```

Screenshot 2: Result- Tampering Percentage

Also it shows the relation between the signature size and the result of proposed system. As the signature size increases from 15 to 90 SIFTs in one signature, the system gives better results. The images get matches and also give better tamper percentage for increased no. of SIFT.



Graph 1- Image matching ratio with Signature size

## V. CONCLUSION AND FUTURE WORK

The schema proposed, is related to the alignment of images in the area of distributed forensic systems. The approach for authentication and the tampering detection of image is proposed using an image registration component which uses an image signature based on the Bag of features concept. It will be difficult to calculate signature in order to change the data as the signature consists of image features and the signature is sent through the trusted server.

The proposed signature uses the spatial distribution of features which can deal with highly texturized and contrasted tampering patches added to the image.

Also histogram of oriented gradients representation is used to perform tampering localization. The system is designed for alignment, authentication and tampering detection using a signature code based on features that are extracted using Scale Invariant Feature Transform.

In future the proposed system can be extended to extract more robust but minimal number of image features needed for accurate estimation of geometric estimation.

## VI. ACKNOWLEDGMENT

This is to acknowledge and thank all the individuals who played defining role in shaping this paper. We avail this opportunity to express our deep sense of gratitude and whole hearted thanks to our friends and family for giving their valuable guidance, inspiration and encouragement to embark this paper.

## REFERENCES

[1] 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.

[2] W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information", in Proc. SPIE Electronic Imaging Symp.-Media Forensics Security, 2010.

[3] W. Lu and M.Wu, "Multimedia forensic hash based on visual words" in Proc. IEEE Computer Soc. Int. Conf. Image Processing, 2010, pp.989,992.

[4] S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering", in Proc. IEEE Computer Soc. Int. Conf. Image Processing,2007, pp. 117-120.

[5] N. Khanna, A. Roca, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Improvements on image authentication and recovery using distributed source coding", in Proc. SPIE Conf. Media Forensics Security, 2009, vol. 7254, p. 725415.

[6] M. Irani and P. Anandan, "About direct methods", in Proc. Int. workshop Vision Algorithms, held during ICCV, Corfu, Greece, 1999, pp. 267,277

[7] 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.

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

[9] S. Battiato, G. M. Farinella, E. Messina, and G. Puglisi, "Understanding geometric manipulations of images through BOVW based hashing", in roc. Int.Workshop Content Protection Forensics (CPAF 2011), 2011.

[10] Photo tampering throughout history [Online]. Available at www.cs.dartmouth.edu/farid/research/digitaltampering/

**Swati S. Bhosale** received the Bachelor degree (B.E.) in Computer engineering in 2005 from VPCOE, Baramati. She is now pursuing Master's degree in Computer Engineering at Vidya Pratishthan's College of Engineering, Baramati. Her current research interests include image processing.

**Gyankamal J. Chhajed has** obtained Engineering degree (B.E.) in Computer Science and Engineering in the year 1991-95 from S.G.G.S.I.E.T, Nanded and Postgraduate degree (M.Tech.) in Computer Engineering from College of Engineering, Pune (COEP) in the year 2005-2007. She is approved Undergraduate and Postgraduate teacher of Pune University and having about 17 yrs. of experience. She guided many projects at Undergraduate and Postgraduate Level. Gyankamal authored a book and has 14 publications at the national, international level for Conferences and Journal. She is life member of the ISTE & International Association IACSIT. Her research interests include Steganography and Watermarking, Image processing, Data mining and Information Retrieval.