Image Registration based on Support Vector Machine for Tampering Localization

Jyoti Rao Sheetal Kusal Swati Nikam Archana Chougule
Dr. D.Y.Patil Institute of Engineering and Technology,
Pimpri, Pune-18

ABSTRACT
Different technologies are available on web. In the era of internet communication, systems should able to protect content such as pictures, videos against malicious modifications during their transmission. One of the important problems addressed in this is the authentication of the image received in a Communication. Tampering detection has significance in authentication of image. This paper presents support vector machine (SVM) based tampering detection system. In this a robust alignment (registration) method is proposed which makes use of an image hash component based on the Bag of Features (BOF) paradigm to localize the tampering. These BOF are clustered for effective image alignment. The support vector machine is optimal partitioning based linear classifier and at least theoretically better other classifier because only small numbers of classes required during classification SVM. The proposed signature is attached to the image before transmission and then analyzed at destination to recover the geometric transformations which have been applied to the received image. A block-wise tampering detection which uses histograms of oriented gradients (HOG) presentation is proposed. The proposed approach obtains better margin in providing an overall enhanced performance by reducing the training time while maintaining the accuracy.

Keywords
BOF, Image Hash, Geometric transformation, image alignment, tampering detection, SVM.

1. INTRODUCTION
The widespread uses of different technologies are available on Internet. In the era of internet systems should able to protect the visual content against malicious modifications that could be performed during their transmission. One of the issues addressed in this is the authentication of the image received in a communication. Altering /manipulating images are not new; it has been around since the early days of photography. Due to the technology, such as digital cameras, powerful PCs and the availability of digital image editing software, image manipulation has become common and easy. Tampering detection is the process of Manipulating, altering, modifying the image for malicious purposes to change meaning of image. Tampering detection falls into two categories as follows: 1) watermarks 2) image hashes. The problem of tampering detection can be addressed using watermarking based approach. A watermark can be inserted into the image and during tampering detection; it is extracted to verify if there was a malicious manipulation on the received image. Damage into the watermark indicates a tampering of the image. A clear disadvantage in using watermarking is the need for distorting the content unfortunately. To overcome this problem signature based approaches have been found. In this approach image hash is not inserted into the image (e.g., in watermarking); it is associated with the image as header information and must be small and robust against different operations. Different hash based approaches have been recently proposed in literature. Most of them share the same basic scheme: i) a hash code based on the visual content is attached to the image to be sent; ii) the hash is analyzed at destination to verify the reliability of the received image. An image hash is a unique signature which represents the visual content of the image in a compact way (just few bytes). An image hash is a short signature of the image that preserves its semantic information under allowable changes made to. That is, it should be robust to allowable modifications and sensitive to distinct images or illegal manipulations to the original like tampering. A common approach of image hashing is extracting features which have perceptual importance. The authentication data are generated by compressing these features or generating their hash values. The user checks the authenticity of the received content by comparing the features or their hash values to the authentication data. In order to perform tampering detection, the receiver should be able to filter out all the geometric transformations added to the tampered image by aligning the received image to the one at the sender.

2. LITERATURE REVIEW
The need of methods useful to establish the validity and authenticity of an image received through an Internet communication is important. To deal with this problem different solutions have been recently proposed in literature [1, 2, 3, 4, 5, and 6]. In [3] propose a robust alignment method which makes use of an image signature based on the Bag of Features paradigm. In [3] Battiato et all proposed a method, an image hash based on the Bag of Visual Words paradigm [4] is attached as signature to the image before transmission. Then forensic hash is analyzed at destination to detect the geometric transformations which have been applied to the received image. In [5] Lin et all proposed a novel approach based on distributed source coding for the problem of backward compatible image authentication. The main idea is to provide a Slepian-Wolf encoded quantized image projection as authentication data. In [6] Lu et all proposed a new framework to perform multimedia forensics by using compact side information to reconstruct the processing history of a multimedia document. They presented a framework as FASHION, stands for Forensic hash for information assurance. There are different robust alignments techniques have been proposed by computer vision researchers [9]-[11]. In [10] Irani and Anandan presented direct Methods which recovers the unknown parameters directly from measurable image quantities at each pixel in the image and direct methods are used for motion or shape estimation. In [9] Torr and Zisserman presented feature based methods where it first extract a sparse set of distinct features from image to build an initial estimation of geometry and then this geometry is used to get of image correspondence in regions of image where there is less information. Richard Szeliski in his tutorial [11], reviews image alignment and image stitching algorithms. But

these techniques are unsuitable in the context of forensic hashing, since a basic requirement is that the image signature should be as compact as possible to reduce the overhead of the network communications. To fit the underlying requirements, Lu et all [6] have proposed to exploit information extracted through Radon transform and scale space theory in order to estimate the parameters of the geometric transformations (i.e., rotation and scale). Lu et all proposed a new framework for multimedia forensics called FASHION. FASHION stands for Forensic hash for information assurance, which bridges two research areas, namely, blind multimedia forensics and robust image hashing, to achieve more efficient and accurate forensic analysis. To make more robust the alignment phase with respect to manipulations such as cropping and tampering, an image hash[7] based on robust invariant features has been proposed by Wenjun Lu and Min Wu in [7]. They proposed a new construction of forensic hash based on visual words representation. They encode SIFT features into a compact visual words representation for robust estimation of geometric transformations and propose a hybrid construction using both SIFT and block-based features to detect and localize image tampering. The technique proposed by Sujoy Roy and Qibin Sun in [8] extends the idea by employing the Bag of Features (BOF) model to represent the features to be used as image hash. The exploitation of the BOF representation is useful to reduce the space needed for the image signature, by maintaining the performances of the alignment component. In [1] the proposed method, an image hash based on the Bag of Visual Words paradigm is attached as signature to the image before transmission. Then forensic hash is analyzed at destination to detect the geometric transformations which have been applied to the received image. This is a more robust approach based on a cascade of estimators has been introduced; it is able to better handle the replicated matchings in order to make a more robust estimation of the orientation parameter. Besides, the cascade of estimators allows a higher precision in estimating the scale factor. A effective way to deal with the problem of wrong matchings has been proposed in [2], where a filtering 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. METHODOLOGY

System consists of two major parts. First part of system consists of alignment component and overall registration framework and second part consists of tampering localization component. Aim of the image alignment component is to model the geometrical manipulations which have been done on the source image during the untrusted communication. Aim of the image alignment component is to model the geometrical manipulations which have been done on the source image during the untrusted communication. Image modifications are estimated by scaling, rotation and translation parameters by using key point co ordinates and hash signatures.

Overall registration is shown in Fig. 1

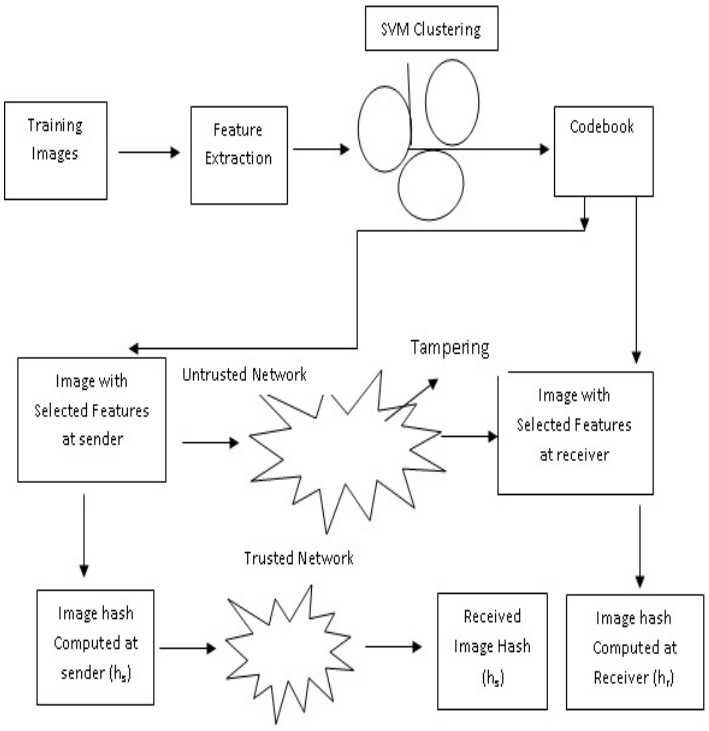

Fig 1: Overall Registration Component using SVM.

System uses a cascade approach; first an initial estimation of the rotation and translation parameters is accomplished through a voting procedure. Afterward, the scaling parameter is estimated by means of the rotation and translation parameters which have been previously estimated on the reliable information [1]. A codebook is generated by clustering set of SIFT [4] features on training images. Clustering points out support vectors. These support vectors represent the codebook to be used during hash generation. This codebook is shared between sender and receiver by trusted network for further use. In [1] Battiato et all adopted K-means clustering for finding centroids and forming codebook for image alignment. As k-means is very classic approach. In our proposed approach we are suggesting SVM on extracted SIFT.

3.1 Support Vector Machine

The key concept of SVMs, which were originally first developed for binary classification problems, is the use of hyper planes to define decision boundaries separating between data points of different classes. The idea behind SVMs is to map the original data points from the input space to a high dimensional, feature space such that the classification problem becomes simpler in the feature space. The mapping is done by proper choice of a kernel function. Illustration of the principles of SVM is shown in figure 2. A main advantage of SVM classification is that SVM performs well on datasets that have many attributes, even when there are only a few cases that are available for the training process.

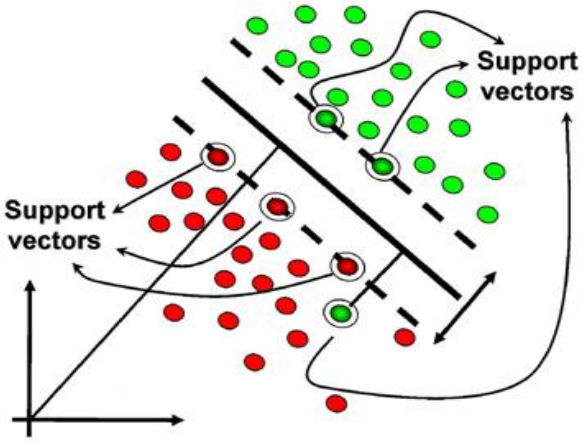

Fig 2: Illustration of the principles of SVM

3.1.1Basic Theory

Consider a training data set D with n points in d dimensional space.

D= xi, yi with i= 1 to n or with xi, yi.

Xi = the input vectors = xi $\in R^d$

Yi = the class labels = yi $\in \{-1, +1\}$.

Yi = the class labels = yi $\in \{-1, +1\}$.

SVM maps the d-dimensional input vector x from the input space to the d_h dimensional feature space using a nonlinear function $\phi(\cdot)$,

$$\phi(\cdot): R^d \rightarrow R^d_h.$$

The separating hyper plane in the feature space is then defined as

$w^T\phi(x) + b = 0$

With b $\in$R and w an unknown vector with the same dimension as $\phi(x)$. A data point x is assigned to the first class, if $f(x) = \text{sign}(w^T\phi(x) + b)$ equals +1

or

to the second class if f (x) equals −1.

Nonlinear function $R^d = d_h$ maps the input space to a so-called higher dimensional feature space. It is important to note that the dimension R^d_h of this space is only defined in an implicit way (it can be infinite dimensional). The term b is a bias term. In primitive weight space the classifier takes the form or it can be written as

$f(x) = \text{sign}(w^T\phi(x) + b)$.

But, on the other hand, is never evaluated in this form. SVM classifier takes the form

$$f(x) = sign(\sum_{i=1}^{\#sv} \alpha i y i K(x, xi) + b)$$

Where #SV represents the number of support vectors and the kernel function K (.,.) is positive definite. Various types of kernel functions can be chosen but we have chosen

Radial basis function (RBF):

$$K(x, z) = \frac{\exp(-\|x-z\|)_2^2}{\rho 2}$$

Where K(*, *) is positive definite for all ρ values in the RBF kernel case.

4. PROPOSED ALGORITHM

The proposed algorithm uses the support vector machine (SVM) for image alignment which is significant in the tampering detection. Proposed systems block diagram shown in figure 3 and can be describe as follows:

Step 1: Read the set of training dataset stored in the database.

Step 2: Extract the SIFT form training dataset.

Step 3: Cluster the training data by SVM.

Step 4: From different support vectors, select the vectors by sorting all SV in descending order and select some first SV to form codebook.

Step 5: store codebook at sender side and receiver side.

Step 6: compute Image Hash (hs) at sender side and Transmit image hash (hs) and original Image to receiver.

Step 7: compute Image Hash (hr) at receiver of received image

Step 8: Compare hr=hs using id values and matching obtained and perform Image alignment by similarity transformation and retrieve the geometric manipulation.

After retrieving geometric manipulation image is analyzed to detect tampered regions by using HOG (Histogram of Gradients) technique.

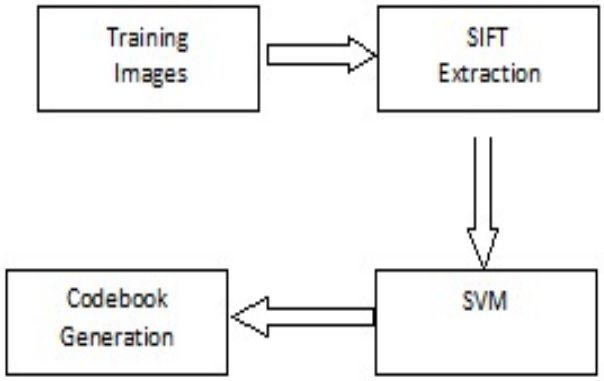

Fig 3: Block diagram of Proposed System

5. RESULTS

This section reports a number of experiments on which the proposed approach has been tested and compared with respect to [1].In our experiments a collection of 15 dissimilar images was used. We have generated perceptually indistinguishable image queries. By performing image transformations as: cropping, rotation, scaling, translation, local tampering, and global tampering. As we are employing overall procedure used by Battiato et al. In [1] Battiato et all performed K-means clustering for forming the codebook. The codebook has been trained through k-means clustering on the overall SIFT descriptors extracted on training images. In our proposed method we are employing SVM clustering. The registration results obtained employing the proposed alignment approach with hash component of different size (i.e., different number of SIFT) are shown in graphs.

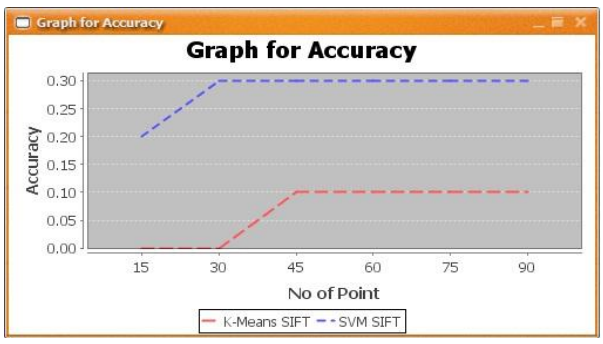

Fig 4: Tampering detection comparison between SVM and k-means. Results have been obtained by increasing number of SIFT points and accuracy.

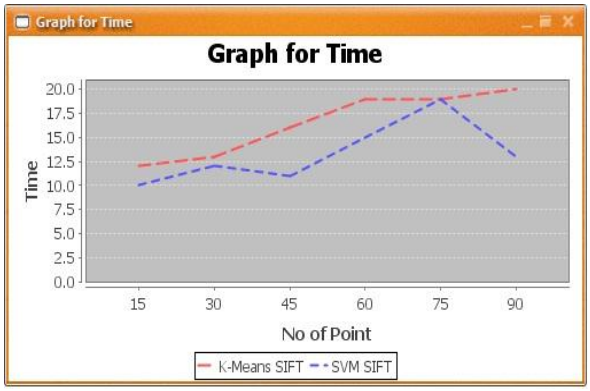

Fig 5: Tampering detection comparison between SVM and k-means. Results have been obtained by increasing number of SIFT points and time.

As shown in Fig.4 by increasing the number of SIFT points the number of unmatched images decreases (i.e., image pairs that the algorithm is not able to process because there are no correspondences between hs and hr). In all cases the percentage of images on which our method is able to work is higher than the one obtained by the approach proposed in [1]. The tests reported in the following reveal that our method strongly outperforms compared to [1] in terms of accuracy and robustness with respect to the different transformations. As time required by SVM is more compared to K-means.(see Fig. 5) But in our method SVM required less time as compared to K-Means. Using SVM clustering, no of SIFT points required are less compared to [1].

6. CONCLUSION

The main contribution of paper related to the alignment of images in the context of distributed systems. A robust image registration component which exploits an image signature based on the Bag of Features paradigm with help of SVM clustering has been introduced. This work is concerned to establish the minimal number of SIFT needed to guarantee an accurate estimation of the geometric transformations by comparing K-means and SVM. The proposed framework by employing SVM is good appeared techniques by obtaining a significant margin in terms of registration accuracy, performances and tampering detection. The proposed approach obtains good margin in providing an overall enhanced performance by reducing the training time while maintaining the accuracy.

7. REFERENCES

[1] S. Battiato, G. M. Farinella, E. Messina,G. Puglisi, "Robust Image Alignment for Tampering Detection, IEEE Transactions On Information Forensics And Security, Vol. 7, No. 4, August 2012

[2] 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.

[3] S. Battiato, G. M. Farinella, E. Messina, And G. Puglisi, "Understanding Geometric Manipulations Of Images Through Bovw-Based Hashing," In Proc. Int. Workshop Content Protection Forensics (Cpaf2011), 2011.

[4] H. Farid, "Digital doctoring: how to tell the real from the fake," Significance, vol. 3, no. 4, 2006.

[5] Y.-C. Lin, D. Varodayan, and B. Girod, "Image authentication based on distributed source coding," in IEEE ComputerSociety International Conference on Image Processing, 2007.

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

[7] W. Lu and M. Wu, "Multimedia forensic hash based on visual words." in IEEE Computer Society International Conference on Image Processing, 2010.

[8] S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering," in IEEE Computer Society International Conference on Image Processing, 2007.

[9] P. H. S. Torr and A. Zisserman, "Feature based methods for structure and motion estimation," in Proc. Int.Workshop Vision Algorithms, held during ICCV, Corfu, Greece, 1999, pp. 278–294.

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

[11] R. Szeliski, "Image alignment and stitching: a tutorial," Foundations and Trends in Computer Graphics and Computer Vision, vol. 2, no. 1, 2006.