INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)

Classification of Copy Move Forgery and Normal Images by ORB Features and SVM Classifier

Er.Nisha
Computer Science Deptt
ACET Bhawanigarh, India
nishamarken@gmail.com

Er. Rajnish Kansal
Computer Science Deptt
ACET Bhawanigarh, India
asra.cse.rajnish@gmail.com

Abstract— the fact that the researcher community recognizes the digital forgery detection need and currently available are very few publications. The mean proposed for fragile authentication, content authentication, tampering detection, localization changes, and original content recovery has been digital watermarks. The image integrity related useful information is provided by the digital watermarks and processing history of it, before the occurrence of tampering the image must have watermark present in it. Their application is limited by this to controlled environments including surveillance cameras or military systems. Unless watermarking chip is equipped in all digital acquisition devices, and watermark can be used for detecting forgery-in the-wild. In this paper use COMFOD dataset by SVM with ORB features

Keywords— copy move forgery, SVM, ORB.

I.INTRODUCTION

The input images are divided into overlapping and regular image blocks by the use of existing block-based forgery detection methods, and then image pixels or transform coefficients matched block by which the tampered regions are obtained; and the key point-based forgery detection methods in which the image key points are extracted and match them for the duplicated regions identification. In this forgery detection method which divides the input image into over-lapping rectangular blocks, from which matches the blocks of the quantized Discrete Cosine Transform (DCT) coefficients for the tampered regions finding. The Principal Component Analysis (PCA) is applied for the reduction of the feature dimensions. In the RGB color components, the direction information as block features is used. The Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) used for the extraction of the image features. Some limitations are there in the existing systems, although in forgery detection, effective are these scheme. Thus, dividing the host image into over-lapping rectangular blocks, computationally this would be expensive as the image size increases. The forgery regions geometrical transformations cannot be significantly addressed by the methods. They have low recall rate because of the regular shape of their blocking method.

1.1.1 Digital Forgeries Detection Need

The powerful programs availability of digital image processing, such as Photoshop, makes the digital forgeries creation relatively from one or multiple images. As shown by the newspaper cut-out, for the creation of the composite image uses three different photographs: The White House, Bill Clinton, and Saddam Hussein images. The White House was rescaled and blurred for an out-of-focus background illusion creation. Then, two different images cuts off the Bill Clinton and Saddam and on the image of the White House, it is pasted.

The fact that sophisticated tools are used for digitally manipulating the images and video to create threatening non-existing situations due to which the credibility and value of presented video tapes and images is diminished in court as evidence independently of the fact either the video is in a digital or analog form. The analog video stream is digitized easily for an analogue video tampering, and uploading it into a computer, forgery is performed, and then the result is saved on an ordinary videotape in the NTSC format. As expected, worse the situation will get as the needed tools by which the forgeries are performed moving from research labs to commercial software.

Despite the fact that the research community recognizes the digital forgeries detection need, and currently very few publications are available. The proposed digital watermarks as a means for fragile authentication, content authentication, detection of tampering, localization of changes, and the original content recovery [1]. While useful information is provided by the digital watermarks about the image integrity and its processing history, there must be present watermark before the tampering occurs in the image. The controlled environments of their application are limited including military systems or surveillance cameras. Unless equipped are these all digital acquisition devices with a watermarking chip, unlikely watermark use can detect a forgery-in-the-wild.

1.2 COPY MOVE FORGERY

Nowadays a variety of applications rely on digital images. These include newspapers, tabloid magazines, scientific Journals, fashion industries, court halls and many others. Today, almost everybody can record, store and share a large amount of digital images because of the spread of easy and cost effective device that enables the acquisition of visual data (Shiva kumar and Baboo, 2011). At the same time, image editing software is widely available which makes it extremely simple to manipulate the content of the image. This can be achieved through creating new images by tampering and counterfeiting the visual content in an expert – like method. Current software allows users to create computer graphics that can't be distinguished from real photos or even to generate hybrid generated visual content (Meyer, et al., 1986). Such developments lead us to ask different forensic – related questions.

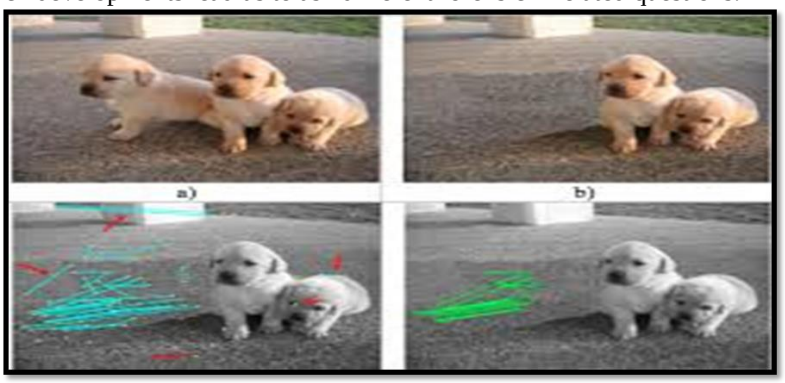


Figure: 1.1 Copy-Move Forgery

The image manipulation of specific type is Copy-Move, where copying a part of the image itself and the same image another part on which it is pasted. Is copy-move forgery example where duplicating a group of soldiers to cover George Bush. Hence, the goal in copy-move forgeries detection is the detection of image areas that are same or extremely similar. The intention of performing the Copy-Move forgery is making an object "disappear" from the image which can be done as the same image parts are copied small blocks are used to cover it. Since the segments that are copied comes from the same image, the color palette, noise components, dynamic range and the other properties which may be compatible with the rest of the image, thus detection for a human eye is very difficult. Sometimes, the forgery detection becomes harder for this technology to detect, if retouched the image with the available tools.

Because of the problem's extraordinary difficulty and largely unexplored character of it, the believe of the authors is that their mechanism categorize forgeries should start research like which starts with the simple ones, and separately each forgery type is analyzed. In doing so, a diverse Forensic Tool Set (FTS) is build. Each tool is though separately considered may not be enough reliable for providing evidence sufficiently for a digital forgery, when the tool complete set is used, the collective evidence is fused by a human expect and hopefully a decisive answer is provided. In this paper, the FTS built towards first step is taken by identifying common forgeries class, the Copy-Move forgery, and efficient algorithms are developed for its detection. In a Copy-Move forgery, itself copying a part of the image and pasted into another same image part. Making an object "disappear" from the image is usual intention of performing by covering it with another image part segment copies. For this purpose, textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal because the background bending likely the copied area and any suspicious artifacts cannot be easily discern by human eye. Because the same image comes the copied parts, its noise component, color palette, dynamic range, and compatible will be most other important properties with the rest of the image and thus by using methods will not be detectable that looked for incompatibilities in statistical measures in image different parts. The forgery is made even harder for detection; either feathered crop or the retouch tool is used for further masking any traces of the copied-and-moved segments.

The original image segment and the pasted one correlation are introduced in Any Copy-Move forgery and for successful detection bases of this forgery type, this correlation is used. Because in the lossy JPEG format likely saving the forgery and because of the retouch tool or other localized image processing tools possible use, but exactly may not match the segments approximately. Thus, the following requirements are formulated for the detection algorithm: 1. For the approximate match of small image segments must be allowed by the detection algorithm 2. While introducing few false positives, a reasonable time is what it must work in (i.e., detection of incorrect matching areas). 3. The connected component will likely be forged segment instead of very small patches or individual pixels collection is another natural assumption that is acceptable.

II. LITERATURE REVIEW

Gomase and Wankhade (2014) [1] In this paper, a technique that is proposed in which intensity of the local changes in the image is found out by applying DWT. For the removal of noise, a median filter is applied. For detection process, dividing the image into overlapping blocks, then storing in a matrix and finally sorting the matrix. Finally, using the matrix by which the copy-move regions are located through pixel matching. This method is useful only when preprocessed are the images, but only copied regions shifting.

Hashmi, et al.(2014) [2] presented a methodology using (DyWT) and (SIFT), which ensures better detection rates after preprocessing and other attacks. First the image is converted to wavelet form (DyWT) for its decomposition into four parts: LL, LH, HL, and HH .SIFT then applied to LL part that most of the information is contained, to obtain the multispectral components and feature vector descriptors. Finally, these feature descriptor vectors is matched is looked for basically for marking the forged regions. The algorithm is simple; showing better detection rates after preprocessing and other attacks can detect more key points for efficient matching. But the False Positive Rate is higher.

Zhao and Guo (2013) [3] This paper proposes a robust method for detection of copy-move forgery which is based on applied to each block. The robust representation is obtained by the quantization of the DCT coefficients which is followed by the quantization blocks division into non-overlapping sub-blocks. On each sub-block applying SVD. Afterwards, each block dimension is reduced with the extraction of features using its largest singular value. Finally, lexicographically sorted are these feature vectors, and matching the duplicated image blocks by shift frequency threshold that is predefined. The results of the experiments show that the copy-move forgery is detected by the proposed method even when an image was distorted by Gaussian blurring; Additive White Gaussian Noise (AWGN), JPEG compression or any other related mixed operations. DCT and SVD.

Al-Sawadi et al.(2013) [4] This paper presented a copy-move image forgery detection method which based on Local Binary Pattern (LBP) and neighborhood clustering. In the proposed method, three color components are what image is decomposed first in. Each component overlapping blocks is used to calculate the LBP histograms. Then calculating the histogram distance between the blocks and retaining the minimal distance in the block-pairs. If the retained block-pairs in all three color components are present and as primary candidates, they are selected. The candidates are refined by applying the eight-connected neighborhood. The results of the experiment show improvement in reducing the false positive rates reduction over some recent methods relation. The methods performance degrades when both rotation and scaling on which pasted part undergo.

Davarzani et al.(2013) [5] In this paper, the method proposed is a tampering detection method which is based on LBP. The copied regions is detected by this algorithm even if the forged region geometry is polluted further by noise, blurring, JPEG compression, scaling or rotation in multiples of 90-degree. In this algorithm the image translation is basically into gray scale and then subdivision is into overlapping blocks. For each block of multi-resolution Local Binary Pattern (MLBP) features are identified by applying the LBP operators of different type. The feature matrices are formed by putting together feature vectors in which the number is equal to the employed number of LBP operators. Lexicographically the feature matrices are sorted and the matching blocks are determined with the use of k-d tree method. Then Random Sample Consensus (RANSAC) algorithm is used for the elimination of false matches. However, it is still a time consuming method. Although reduced complexity is in this method and for large block size is highly discriminative, reducing its accuracy considerably for small block sizes and in high resolution images for forgery detection having low JPEG qualities, and the duplicated regions cannot be detected with arbitrary rotation angles either.

Zhong and Xu (2013) [6] This paper presented mixed moments based method. First, uses the Gaussian pyramid transform for the extraction from the image of the low-frequency information then divided it into overlapping blocks; Secondly, the exponenti-fourier moments composes the block eigenvector and lexico graphically sorted is the histogram moments; thirdly, precisely positioning the tampered region and quickly to the Euclidean distance and space distance accordingly. The results of the experiment shows that successfully this method forged part can detected with translation, rotation, scaling and mixed operation tamper when the brightness variation and contrast adjustment changing the image. But not specifying the qualitative evaluation, rotation angle and scaling factor.

Muhammad (2013) [7] In this paper, a multi-scale local texture descriptor is proposed for image forgery detection. (Hussain et al., 2012) presented the same approach, but with the applying difference of the un-decimated wavelet transform for the channel extracting the lower sub-band. Before doing that, the chromatic channel is into which it is decomposed on an input image. The proposed multi-scale local texture descriptor, called Weber Pattern (WP) which is inspired by the Weber's Law and from the sub-band is calculated. The image feature is the consideration of the WP histogram. In the framework, support vector machine as a classifier is used. The result of the experimentation on different image datasets shows the superiority which is in terms of accuracy. In addition, the accuracy achieved in this method is 92.28% for showing toughness of JPEG compression against Q factor.

Amerini et al.(2013) [8] In this paper, for feature extraction a Scale Invariant Feature Transform (SIFT) is employed, the J-Linkage algorithm bases localization combined for detecting tampering. For the image extracting the SIFT features. The g2NN algorithm is used for the matching of the feature vectors afterwards. Considering the matched vectors coordinates likely candidates for clustering, in which J-linkage algorithm is used for performing. The copied regions reveal the clustering result. Because the SIFT features are adopted by the method, it has capability of forgeries detection involving scaling and rotation. Multiple duplications are detected successfully in this method and the tampering regions are also localized with a precision high degree.

III. METHODOLOGY

Step1: Input the different types of images.
Step2: Extract different type of features.
Step3: normalize the features by scaling method.
Step4: Matching using ORB features (Oriented FAST & Rotated BRIEF).
Step5: Classification by reducing the false positive error.
Step6: Post processing by analysis precision, recall, accuracy.

IV. RESULT AND DISCUSSION

Table 1: 600 Images +ORB Features

Classifier	Accuracy (ORB)	Precision(ORB)	Recall (ORB)
SVM+RBF	90.24	87	83
SVM+EM	97	82	87

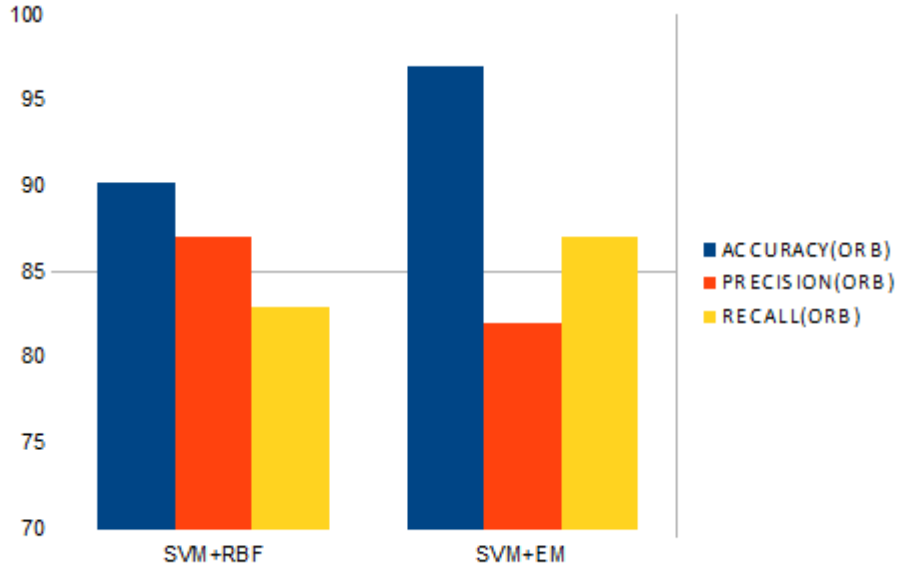


Table 2: 600 Images +SIFT Features

Classifier	Accuracy(SIFT)	Precision(SIFT)	Recall(SIFT)
SVM+RBF	87.5	87.25	87.5
SVM+EM	94.57	82	90

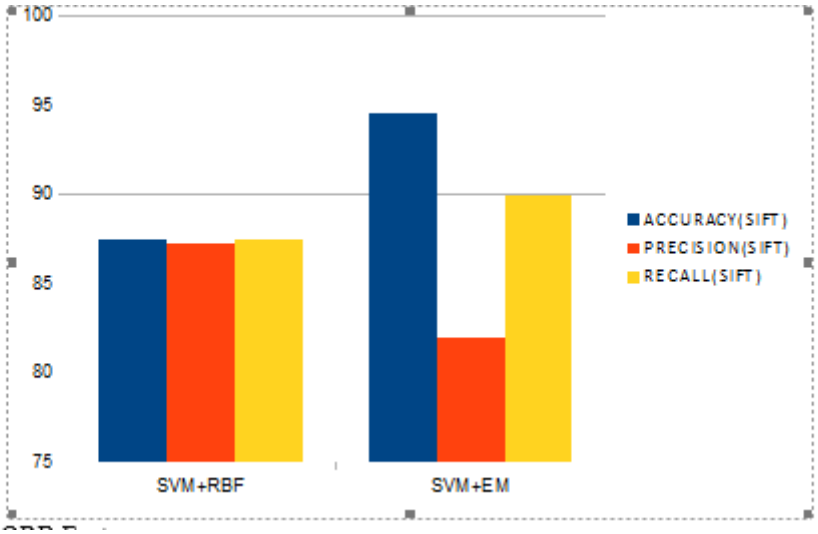


Table 3: 300 Images +ORB Features

Classifier	Accuracy(SIFT)	Precision(SIFT)	Recall(SIFT)
SVM+RBF	93.14	85	90
SVM+EM	94	89	90.23

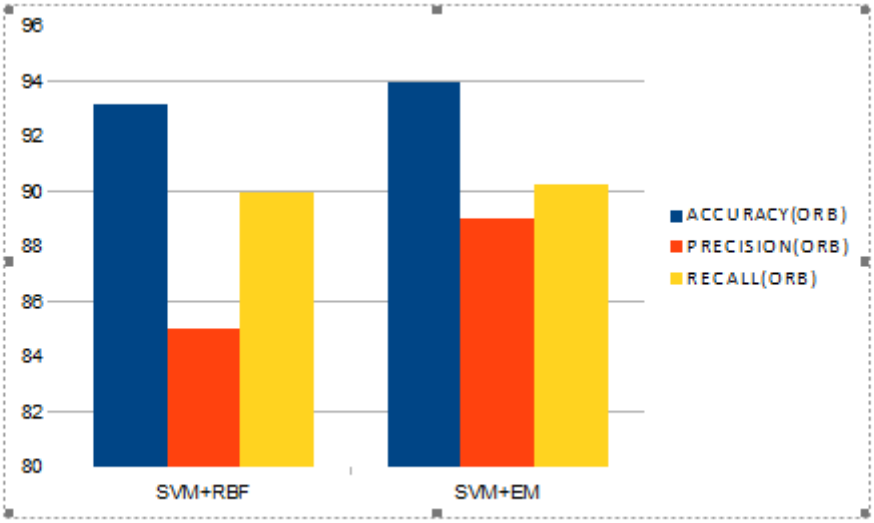


Table 4: 300 Images +SIFT Features

Classifier	Accuracy(SIFT)	Precision(SIFT)	Recall(SIFT)
SVM+RBF	62.5	61	83
SVM+EM	83.1	72	75

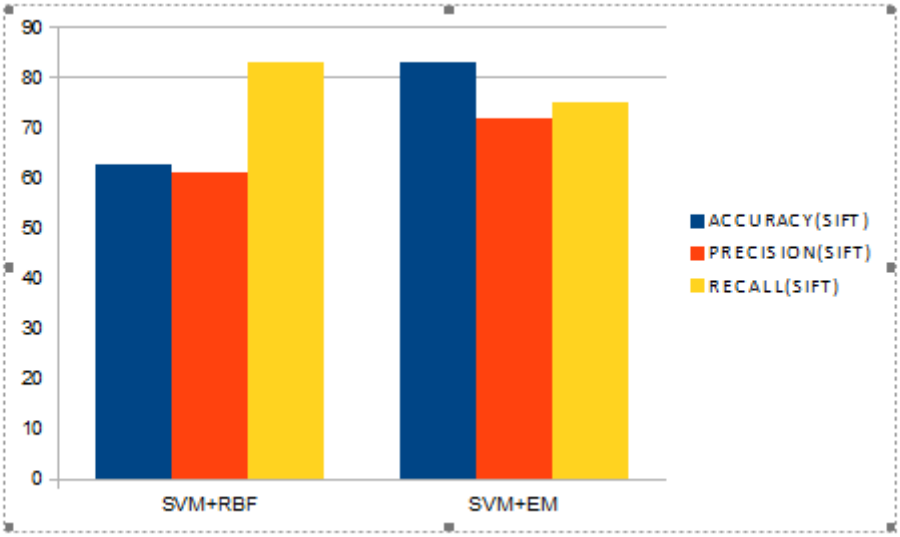
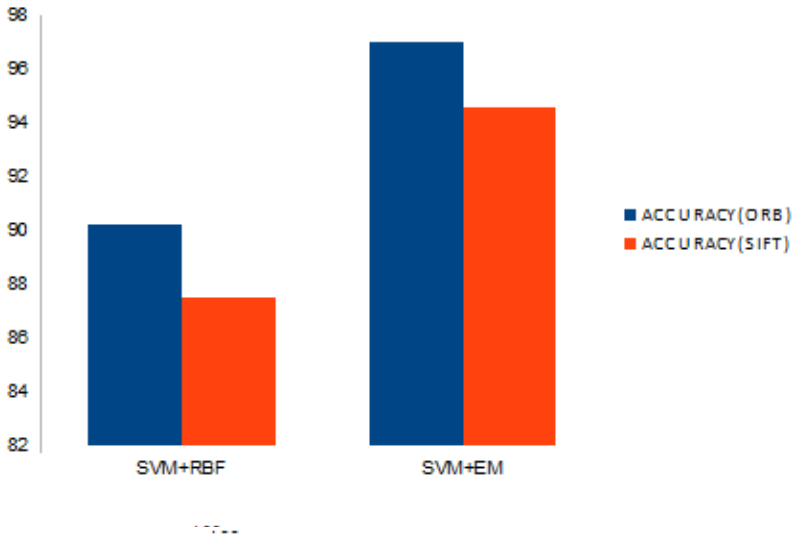
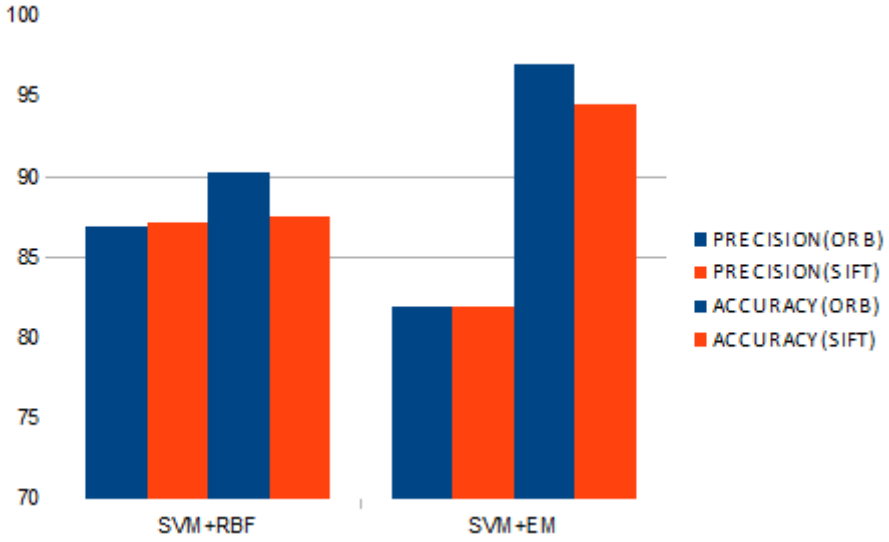
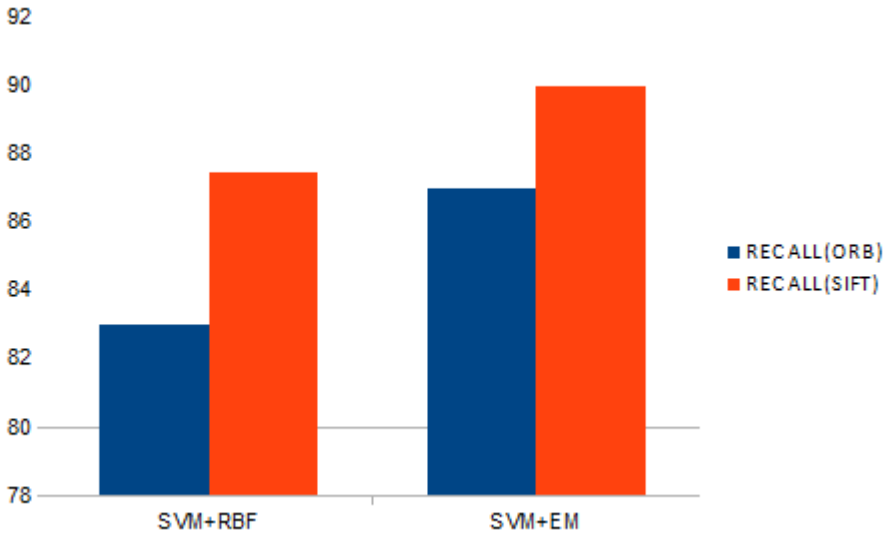


Table 5: Comparison Between Precision, Recall &Accuracy of 600 Images

Classifier	Accuracy (ORB)	Accuracy (SIFT)	Precision (ORB)	Precision (SIFT)	Recall (ORB)	Recall (SIFT)
SVM+RBF	90.24	87.5	87	87.25	83	87.5
SVM+EM	97	94.57	82	82	87	90







Among proposed features, one is sift which is not based on orientation but this is a point wise feature and other features are ORB features which depend on orientation on different angle. In classifier one, other optimization are not in optimization base using exception maximization which is an iterative optimize. Therefore, in result Orientation based

feature give better result than both classifier but if we compare the classifier then optimization classifier plays an important role.

CONCLUSION AND FUTURE SCOPE

With the image processing technology rapid progress, an interesting research topic is the digital image forgery detection in forensic science. Considering the image tampering specific type as a "copy-move forgery", this is an emerging problem in the digital image forensic field. An original digital image part is copied and pasted in the same original image another part to make it a copy forged one in copy-move forgery method. The classifications of "Copy-Move Forgery" are based on ORB and SIFT Features. In this thesis, classifier of different types are used like SVM and EM algorithm in which the copy image and original image are classified and that gives higher accuracy and precision and recall.

Based on the improved method performance in digital images for "copy move forgery classification", This research extensions is highly recommended in the future to: Problems like rotation and scales are dealt. The multiplex forensic tools in conjunction is the future digital forensic direction with the sensible policy and awareness and law that create convincing digital forgeries.

REFERNCES

[1] A. Fridrich, et al., Detection of Copy-move Forgery in Digital Images, 2003.

[2] Y. Huang, et al., Improved DCT-based detection of copy-move forgery in images,Forensic Science International 206 (1–3) (2011) 178–184.

[3] A. Popescu and H. Farid, Exposing digital forgeries by detecting duplicate image regions, Dept. Computer. Sci. Dartmouth College, Tech.Rep. TR2004 515, 2004.

[4] B. Mahdian, S. Saic, Detection of copy-move forgery using a method based on blur moment invariants, Forensic Science International 171 (2007) 180–189.

[5] Li Jing, and Chao Shao," Image Copy-Move Forgery Detecting Based on Local Invariant Feature Journal Of Multimedia,Vol.7,No.1, February 2012.

[6] Vincent Christlein," An Evaluation of Popular Copy-Move ForgeryDetection Approaches", IEEE Transactions On Information Forensics And Security, 2011.

[7] S. Bayram, H.T. Sencar, N. Memon," An efficient and robust method for detecting copy-move forgery", in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York, 2009.

[8] X. Pan, S. Lyu," Detecting image region duplication using SIFT features", in: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP),2010, 2010, 1706–1709.

