INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue4)
Available online at www.ijariit.com

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

Rekha Devi
Yamuna Group of Institutions(Haryana)
rekhakashyap80@gmail.com

Deepti Chauhan
Yamuna Group of Institutions(Haryana)
maildeepti67@gmail.com

Abstract: Today, the characterization of the technological age is done by the digital images spread. They are the most common form of conveying information whether through internet, newspapers, magazines, or scientific journals. They are used as a strong proof of various crimes and as evidence used for various purposes. The modification, capturing or creating of the image has become easier and available with the emergence of means of image editing and processing tools. One of the most important and popular types of image forgery is a copy-move forgery in which an image part is copied and then pasted into the same image that has the intention of hiding something important or showing a false scene. Because the important properties of the copied parts come from the same image, such as brightness, noise, and texture which will be compatible with the entire image that makes more difficult for experts for the detection and distinguishing the alteration. Usually, the detecting copy move forgery conventional techniques suffer severely from the time-consuming problem. The evaluation of the improved method had been done using (150) images that were selected from two different datasets, "CoMoFoD" and "MICC-F2000". Experimental results show that the improved method can accurately and quickly reveal the doubled regions of a tampered image. In addition, greatly reducing the processing time in comparison to the Khan algorithm, and the accuracy is kept at the same level. Owing to the availability and technological advancement of the image editing sophisticated tools, there is an increase in the loss of authentication in digital images. Thus, this led us to the proposal of different detection techniques that checks whether the digital images are forged or authentic. The specific type of forgery technique is copy move forgery in which widely used research topic is detection under digital image forensics. In this thesis, an enhancement of copy move image forgery classification is done by implementing hybrid features with classification algorithms like SIFT with SVM and EM algorithm and ORB with SVM and EM.The technique works by applying Firstly the DCT on an image and then on a resultant image, SIFT is obtained after applying DCT. A supervised learning method is proposed for classifying a copy-move image forgery of TIFF, JPEG, and BMP. The process starts with reducing the color of the photos. Achieve the accuracy more than 90%.

Keywords: DCT, COMFOD, SVM, EM, RBF, SIFT, ORB.

I. INTRODUCTION

Nowadays, a variety of applications relies on digital images. These include tabloid magazines, fashion industries, scientific Journals, court halls, newspapers and many others. Today, digital images of a large amount can be stored, shared and recorded almost by everyone because of the easy spread of device that is cost effective enabling the visual data acquisition (Shivakumar 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 new images created in an expert – like method by counterfeiting and tampering the visual content.

The image manipulation specific type is copy-move, where the same image part is copied and then on another part of the same image is pasted. As the copy-move forgery example, for covering George Bush duplicating the soldier's group. Fundamentally, digital images consist of the picture elements (pixels) combination. These individual pixels are brightened and colored for the generation of a digital picture which is logical state arrangement of a slew of pixels. The amount of pixel embodies of red, green, and blue corresponds to each octet with an 8-bit number represents most color images. A grayscale image typically contains one 8-bit number to signify the amount of gray in a pixel.

The image processing is exploited by a new discipline known as digital image forensic and an image history information recovered by the analysis tools. Any digital image trustworthiness must be ensured when any piece of information is conveyed by the use of an image. The trustworthiness of any image may verify the authenticity of the image which means that such image was not manipulated or counterfeited indicating a valid representation of the real world (Zhao and Guo, 2013).

The main purpose of forgery analysis is to determine whether any changes were made to change the meaningful content of an image (Vijayaraghavan, 2014). Is every altered image a forged one? Digital image forgery means the intentional manipulation of the digital image, for the purpose of changing the semantic meaning of the visual message included in that image. There are some techniques applied to the image such as cropping, rotating or applying horizon correction which are widely accepted techniques since they alter the image without necessarily forging it (Al-Sawadi, 2013).

The image forensics main goal is the Image forgery detection since as evidence digital images were presented in courts of law, as a financial document as a medical records part, or news items.

II. LITERATURE REVIEW

(Fredrich, et al., 2003) In this paper, a method is proposed for the detection of copy- move forgery. The computational burden is avoided by considering their lexicographical sorting and using the image blocks having Discrete Cosine Transform (DCT). Once sorted, the copy-moved blocks are considered as the adjacent identical pair of blocks. The small duplicate regions cannot be detected that is this method's drawback.

Cao et al. (2012), present region duplication detection algorithm which depends on improved DCT and exhibits low computational complexity. The profound difference between this method and the other DCT-based methods is that here the quantized block is characterized by a circle block. Then, dividing the circle block into a fixed number of parts, for which calculating the feature vectors. Euclidean distance between adjacent pairs is calculated after lexicographic sorting of vectors. The actual distance between the similar vectors is also considered before the final call on duplication is made. This method is capable of identifying multiple region duplications and is also robust against blurring and additive noise but it has poor performance with poor image quality. It is not robust to geometrical operation either.

Zhao and Guo (2013), In this paper, a robust method is proposed for the detection of copy-move forgery on the basis of applying to each block. The DCT coefficients are then quantized to obtain a more robust representation of each block followed by dividing these quantized blocks into nonoverlapping sub-blocks. SVD is applied to each sub-block. Afterward, features are extracted to reduce each block dimension using its largest singular value. Finally, feature vectors are lexicographically sorted, and the duplicated image blocks are matched by predefined shift frequency threshold. The results of the experiment show that copy-move forgery can be detected by the proposed method even when distorted is the image by Additive White Gaussian Noise (AWGN), Gaussian blurring; or any other related mixed operations.

Popescu and Farid (2004) suggested a method using Principal Component Analysis (PCA). In this method, firstly transforming the image into grayscale and then separated into many parts which are represented by vectors. These parts or blocks are organized lexicographically and PCA is used to represent the dissimilar blocks in a substitute mode. It is proficient for detecting even minor variations resulting from noise or wasted compression. Moreover, this technique is far efficient for gray scale images. It is better for detecting copy-move forgeries and gives less number of false positives. The computational cost and the number of computations required are considerably reduced O(NtN logN), where Nt is the dimensionality of the truncated PCA representation and N is the number of image pixels.

Al-Sawadi et al. (2013), presented a copy-move image forgery detection method based on Local Binary Pattern (LBP) and neighborhood clustering. Firstly, in the proposed method an image is decomposed into three color components. Then, calculating LBP histograms from each component overlapped blocks. The minimal distance between the block-pairs is retained and then, calculating the histogram distance between blocks. In all the three color components, if the block-pairs that are retained are present in which they are selected as primary candidates. Eight-connected neighborhood clustering is then applied to refine the candidates. The results of the experiment show the improvement for the reduction in the false positive rates over some related methods. The performance of the methods degrades when the pasted parts undergo both rotation and scaling.

Davarzani et al. (2013), proposed a tampering detection method based on LBP. The copied regions can be detected with this algorithm even if the forged region geometry is polluted further by blurring, noise, scaling, in multiples of 90-degree rotation or JPEG compression. In this algorithm, the image is translated into gray scale and is then subdivided into overlapping blocks. LBP operators of different types are applied for the identification of Multi-resolution Local Binary Pattern (MLBP) features for each block. To form feature matrices putting together the feature vectors in which the number is equal to the employed number of LBP operators. Feature matrices are lexicographically sorted and k-d tree method is used for determining the matching blocks. The random SAmple Consensus (RANSAC) algorithm is then used to eliminate false matches. However, the method is still time-consuming Although this method has reduced complexity and is highly discriminative **for** large block size, its accuracy is reduced considerably for small block sizes and low JPEG qualities for forgery detection in high-resolution images, and it cannot detect duplicated regions with arbitrary rotation angles either.

III.PROPOSED METHODOLOGY

The image manipulation specific type is copy-move, where the same image part is copied and then on another part of the same image is pasted. Take the different types of images and Extract feature of different types of the image by using point scale or block scale method after that normalize the features of all taken images by scaling method. Matching features of images by using ORB features (Oriented FAST & Rotated BRIEF).Then Classification of images by reducing the false positive error and Post processing by analysis precision, recall, accuracy has been compared in this work

IV.RESULT AND DISCUSSION

Table 3.1: 600 Images +ORB Features

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

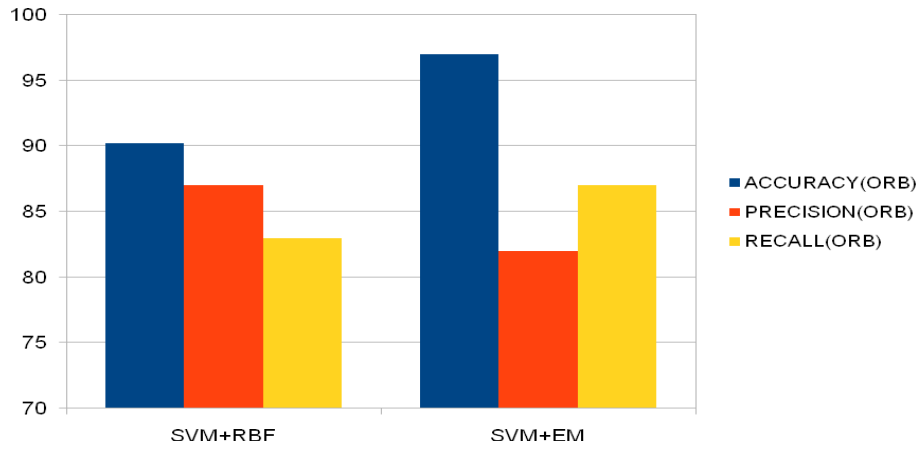


Table 3.2: 600 Images +SIFT Features

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

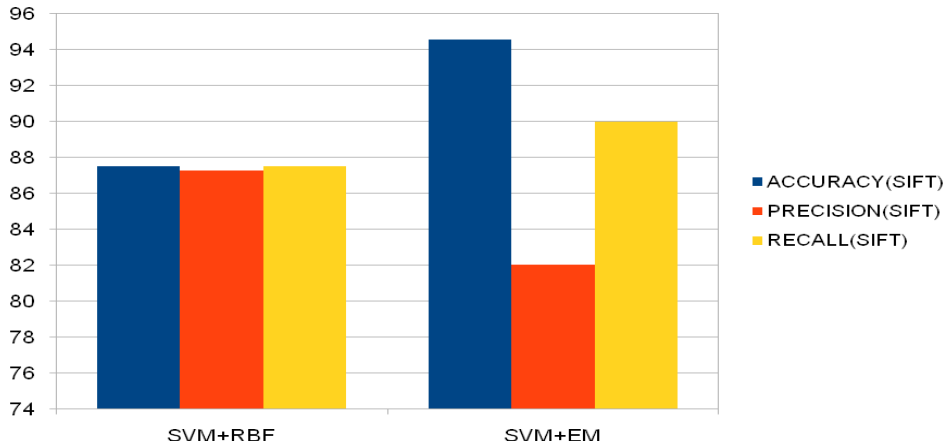


Table 3.3: 300 Images +ORB Features

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

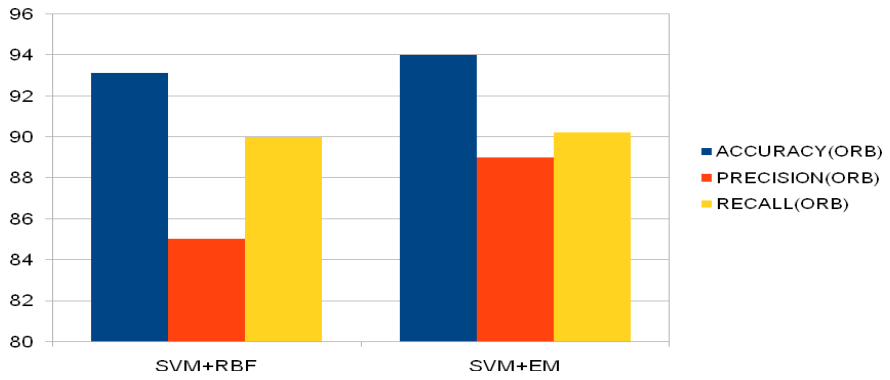


Table 3.4: 300 Images +SIFT Features

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

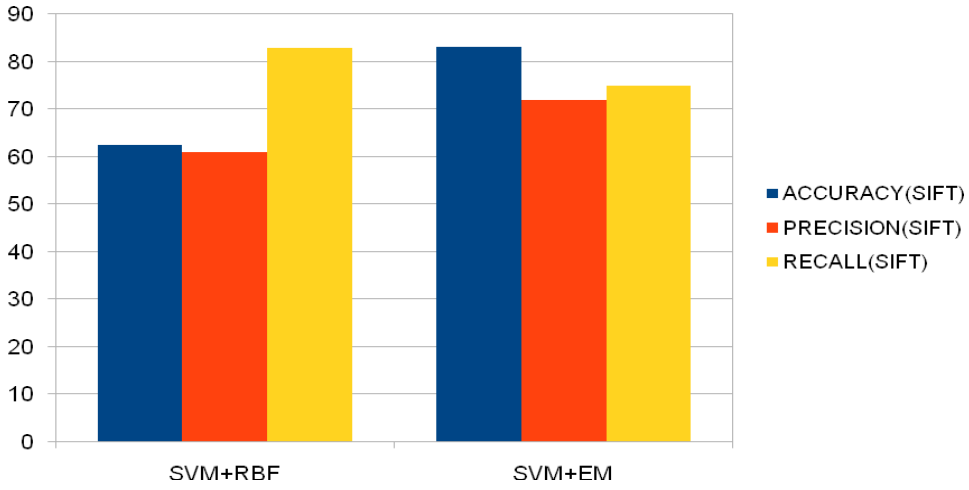
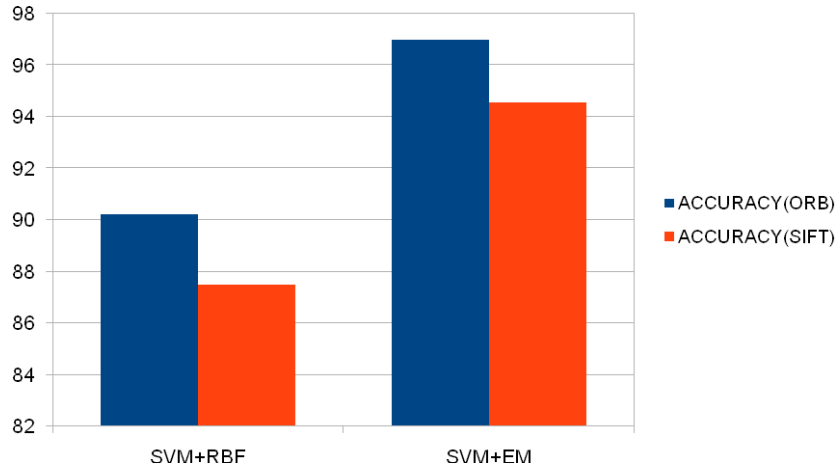
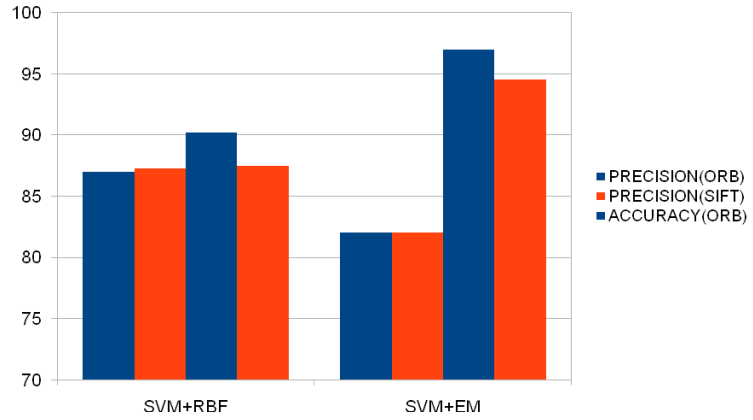


Table 3.5: Comparison between Precision, Recall &Accuracy of 600 Images

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





CONCLUSIONS

We can consider the specific type of image tampering as a "copy-move forgery", which is one of the emerging problems in the field of digital image forensic. It has successfully demonstrated the strengths and weaknesses of three distinct image forgery detection algorithms, and their ability to perform on a large sample set of both unique sample sets and dataset image libraries. Image Resampling Detection provided a robust solution for detecting resampling distortions within the underlying frequencies of the image. Success rates were similar between both the unique forged image set and the image manipulation dataset. In copy-move forgery method, a part of the original digital image is copied and pasted to another part in the same original image to make it, as a copy forged one. "Copy-Move Forgery" classification based on SIFT and ORB Features. In this thesis used a different type of classifiers like SVM and EM algorithm which classifying the images in copy and the original image, which give higher accuracy and precision and recall.

FUTURE SCOPE

Along with so many advantages, the tool, of course, has some drawbacks observed during implementation and testing.

- The tool depends on some input parameters which are assumed constant, but in reality, they can be optimised.
- In copy-move tamper detection, if the number of tampered regions is more than one, then the current algorithm is able to detect only the region which is larger in size.
- Detection of noise variance in an image with the implemented algorithm only works if the added noise has a standard deviation greater than a value of 10. Much work is needed to be done in this field of image forensics based on image data analysis and observation, as tools for image tampering or enhancement are already mature, but detection tools are still in infancy stage. As a future work, the implemented software can extend by
- Adding the capability of detecting multiple copy-move tampering in a single image. This can be done by classifying shift indexes of the blocks calculated after lexicographic sorting and quantizing.
- Input parameters can be optimized by testing with a large database of images and observing more over the influence of these parameters on the performance of the algorithms
- By implementing more detection algorithms into the tool, a classifier based on ranking the predictions of the detection algorithms can be built to tell precisely the existence of tamper detection.
- Based on the performance of the improved method for "copy move forgery classification" in digital images, we can highly recommend extending this research in the future to:
- Deal with a problem such as rotation and scales.
- Work on videos where the search for duplicated blocks to perform on multiple image frames.
- The future digital forensic direction would be multiplex forensic tools in conjunction with awareness and sensible policy and law that create convincing digital forgeries

REFERENCES

[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 SIFTfeatures", in: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP),2010, 2010, 1706–1709.
[9] Frank Y. Shih and Yuan Yuan,"A Comparison Study on Copy-Cover Image Forgery Detection", The Open Artificial Intelligence Journal, 2010, 4, 49-54.
[10] Preeti Yadav, YogeshRathore, Aarti Yadav," DWT Based CopyMove Image Forgery Detection", International Journal of Advanced Research in Computer Science an Electronics Engineering Volume 1, Issue 5, July 2012
[11] Hwel-Jen Lin, Chun-We Wang," Fast Copy-Move Forgery Detection", WSEASTransactions on SIGNAL PROCESSING, May 2009.
[12] B.L.Shivakumar1 and Lt. Dr. S.SanthoshBaboo," Detection of Region Duplication Forgery in Digital Images Using SURF", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.
[13] Muhammad, Ghulam, Muhammad Hussain, and George Bebis. "Passive copy move image forgery detection using undecimated dyadic wavelet transform." *Digital Investigation* 9.1 (2012): 49-57.
[14] Al-Hammadi M. (2013), Copy Move Forgery Detection In Digital Images Based On Multiresolution Techniques, Master Thesis, Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh.
[15] Al-Qershi, O. and Khoo, B. (2013), Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art, Forensic Science International, vol. 231, Issues 1-3, pp. 284–295.

