"IMAGE FORGERY DETECTION USING SUPPORT VECTOR MACHINES: DEVELOPMENT AND EVALUATION"

Ekta Bala

Ekta6535@gmail.com

Department of Computer Science and Engineering, SBSSU Gurdaspur

Abstract

The revolution in digital imaging technologies has changed our lives. In comparison to textual information, information through an image is more direct and instant. With the help of sophisticated software, a real-like image can be generated and a real photographic image can be manipulated. Hence it is possible that some image forgers can maliciously tamper the digital image to distort the truth. To restore trust in digital images, the investigation of forgery in images is essential. When the content of a digital image is modified or the whole image is created using a computer graphics software for wrong motives, such an image is commonly referred to as a forged image, and the process of creating such forged image is known as digital image forgery. In this dissertation, a systematic and complete solution is provided to authenticate a digital image. For this, two commonly performed image forgery types viz. copy-move forgery and image splicing forgery have been investigated in this thesis. Further, it is also required to develop are liable method to detect image forgery in photographic images. Various concepts such as Tetrolet transform, Gaussian-Hermite moments, Neuro-fuzzy classifier, etc. are explored and used in the proposed approaches. Experimental validation of all the proposed methods has been performed on various available image datasets and the results are compared to the existing technique on the behalf of certain performance parameters including Compression, Robustness, Accuracy and F1 score.

CHAPTER 1
INTRODUCTION

1.1 Preamble

Images and videos are the most effective means to communicate information because of their expressive potential. Availability of high quality and low-cost recording devices and efficient communication systems have resulted wide use of the digital images and videos. Print and electronic media use images or videos to present information vividly. For a long time, images and videos were generally accepted as proof of occurrence of events. Many decisions are being made in Government, Legal organizations and scientific institutions, taking digital multimedia content asevidence.

1.2 Photography and Digital Images

The history of photography dates back to 11th century to the development of pinhole camera called obscura (dark room) and has seen continuous developments in the imaging technology. Till the previous decade, photos were captured on films which had be developed to get the negative and using them the photos (positives)were printed. This used to be time consuming as well as costly. Videos were captured on magnetic tapes and had to be recorded and played by special devices.

The general structure of a digital camera is shown in Figure 1.1. Digital cameras consist of Lens System, Filters, Color Filter Array (CFA), Image Sensor, and Digital Image Processor (DIP) [1].

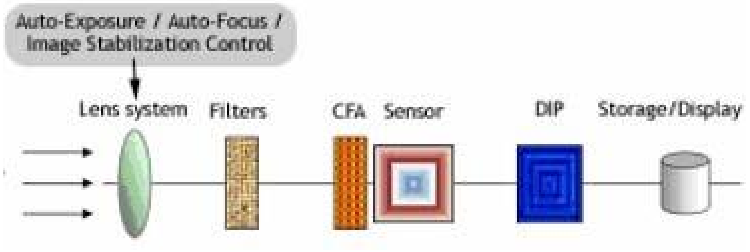


Figure 1.1: Structure of a Digital Camera

Colour images may suffer from chromatic and spherical aberrations caused by the lenses. Chromatic aberration is the failure to converge light of different wavelengths at the same position on the sensor. Spherical aberration causes light passing through the periphery of the spherical lens to converge at a point closer to the lens than light passing through the center of the lens. These effects can be minimized using special combinations of convex and concave lenses, as well as using aspheric lenses. The Lens System also includes the Auto-exposure Control, Auto-focus Control and the Image Stabilization Unit. Auto-exposure Control along with a calibrated Automatic Gain Controller, changes the aperture and the shutter speed to capture well exposed images. Auto-focus Control runs a miniature motor that focuses the lenses bymoving them in and out until the sharpest possible image is obtained. Image Stabilization Unit counteracts camera shake and helps to get sharper pictures.

After passing through the lenses, light goes through a set of filters. Aninfrared filter is an absorptive or reflective filter allowing only the visible part of the spectrum to pass, while blocking infrared radiation that can reduce the sharpness ofthe formed image. An anti-aliasing filter reduces aliasing, a phenomenon that happens when the spacing between pixels in the sensor cannot support the finer spatial frequency of the target objects such as decorative patterns. At the heart of a digital camera is the Image Sensor which is an array of photodiode elements, or pixels. When light strikes the pixel array, each pixel generates an analog signal proportional to the intensity of light, which is then converted to digital signal and processed by the DIP. Most digital cameras use a Charge-Coupled Device (CCD) as the image sensorial though CMOS chips are a popular alternative. Sensor pixels are not sensitive to colours; they just record the brightness of light, thus producing a monochromatic output. To produce a colour image, a colour filter array (CFA) is used in front of the sensor so that each pixel records the light intensity for a single colour only. Most digital cameras use the Green-Red-Green-Blue (GRGB) Bayer pattern CFA. The output from the sensor with a Bayer filter is a mosaic of red, green and blue pixels of different intensities. Since each pixel records only one of the three colours, the full colour image is accomplished by the DIP using various interpolation (mosaicking) algorithms. Other alternative CFA filters include the Cyan-Yellow-Green-Magenta (CYGM) pattern, the Red-Green-Blue-Emerald (RGBE) pattern, and the Cyan- Magenta-Yellow (CMY) pattern. DIP also performs further processing such as white balancing, noise reduction, matrix manipulation, image sharpening, aperture correction, and gamma correction to produce a good quality image.

1.3 Image Forgeries

Shortly after the advent in 1814, photography became the chosen method for making portraits, and portrait photographers learned that they could improve sales by retouching their photographs to please the sitter. Later, attempts have been made to alter an image and modify its contents. Many such cases have been notorious that raise ethical questions. Three samples have been shown in Figure 1.2, 1.3 and 1.4 [2]

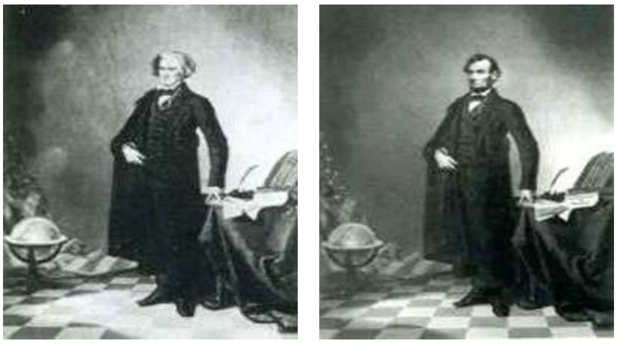


Figure 1.2: Abraham Lincoln's head has been superimposed onto a portrait of the southern leader John Calhoun. (Circa-1860).

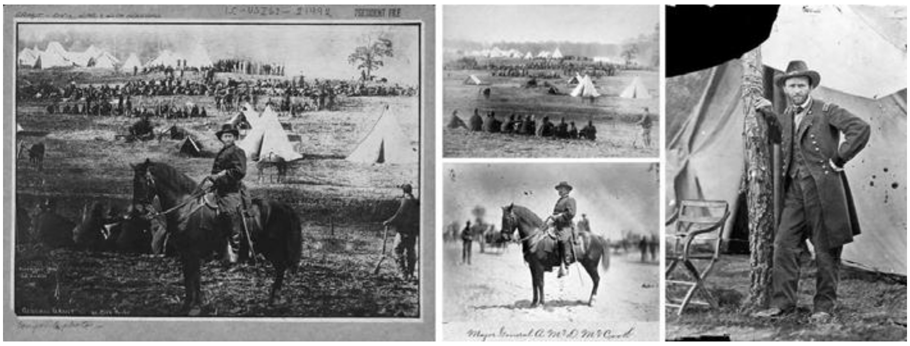


Figure 1.3 : The photo of General Ulysses S. Grant in front of his troops during the American Civil War - Identified to be a composite of threephotographs. (Circa-1864).

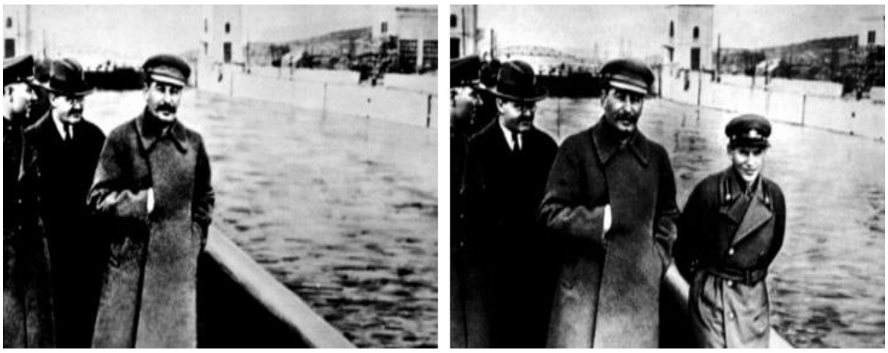


Figure 1.4: Stalin routinely air-brushed his enemies out of photographs. Nikolai Yezhov has been removed here. (Circa 1930)

With the development of digital photography, high performance computers, low-cost and sophisticated, editing and computer graphics software, digital images and videos are very easily manipulated and altered. The process of altering an image and presenting it as the true copy of the original is termed Digital Image Forgery.

1.4 Image Editing

An image can be modified with different objectives. If it is for improving it quality of depiction it can be considered as innocent. If it is done with an intention of modifying the content that alters the information conveyed by the original, it isconsidered as malicious. Three types of modifications/ editing can be done on images [5]:

- Enhancement
- Geometric modification, and
- Content modification.

Geometric modifications can be innocent or malicious. Content modification istermed as forgery. Figure 1.5 shows the three modifications each with a set of editing operations. Image forgery may include a combination of these operations also.

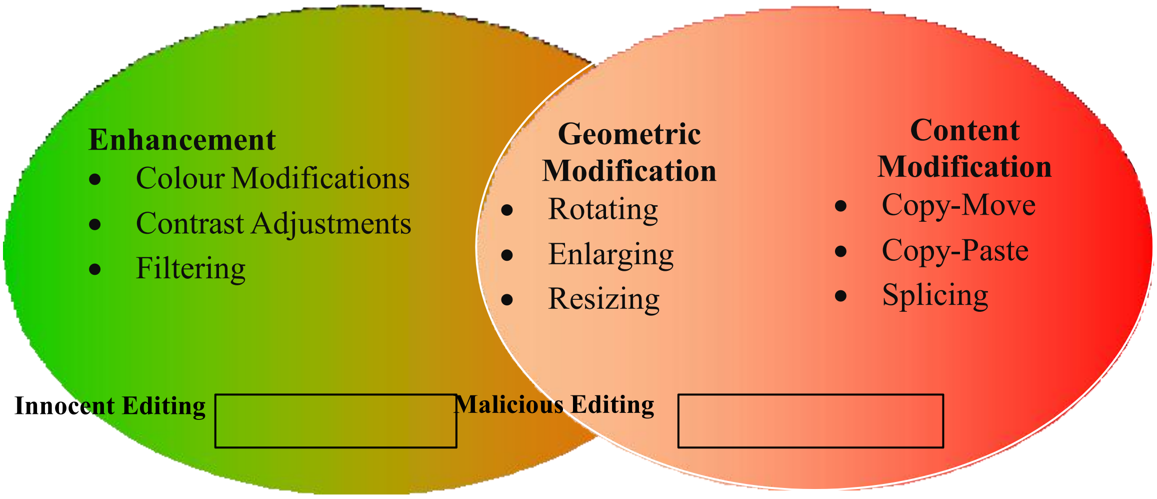


Figure 1.5 : Image Editing Operations

1.5 Image Forgery

Normally, image forgery is done to conceal an object in an image, duplicate one or more objects in the image or insert object(s) picked from one or more images. Generally, there are three main types of forgeries.

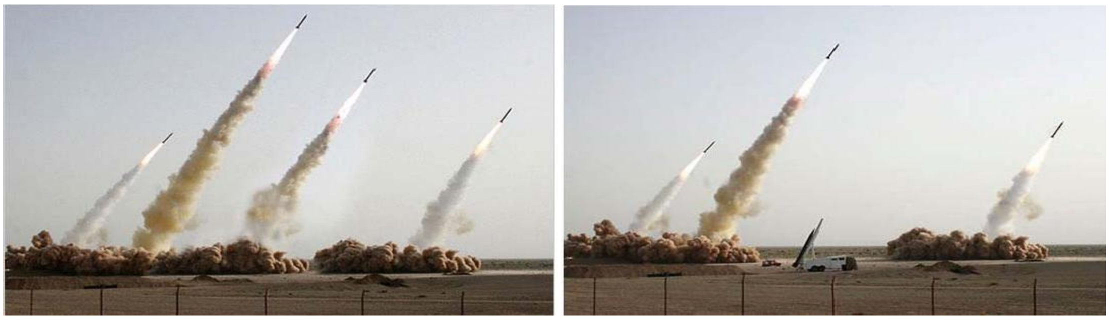


Figure 1.6 : Copy-Move Forgery/ Cloning : (Left) Image that Agence France- Presse obtained from Sepah News, of Iran's Revolutionary Guard on 09/07/2008. (Right) Original Image that *The Associated Press* received from the same source on 10/07/2008

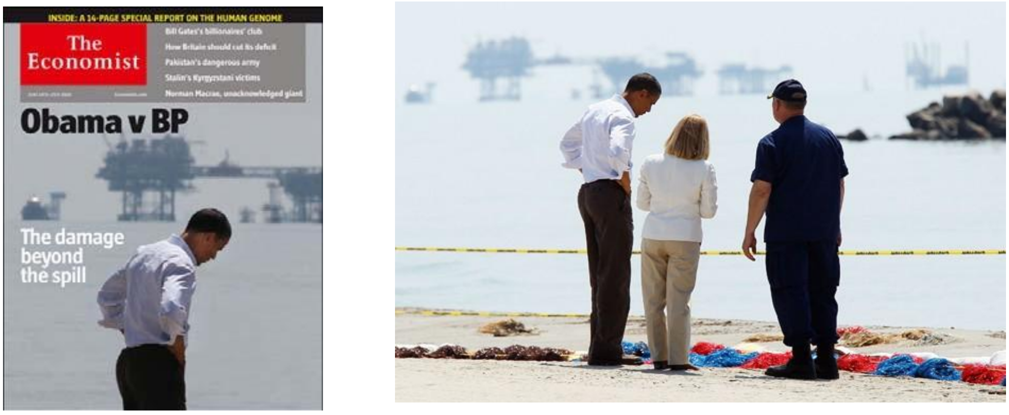

INSIDE: A 14-PAGE SPECIAL REPORT ON THE HUMAN GENOME
The Economist
Bill Gates's billionaires' club
How Britain should cut its deficit
Pakistan's dangerous army
Stalin's Kyrgyzstani victims
Norman Macrae, unacknowledged giant
Obama v BP
The damage beyond the spill

Figure 1.7 : Copy-Move Forgery/ Cloning: Photo of Obama on a Louisiana beach with colleagues. For its cover image, The Magazine – theEconomist, showed only Obama

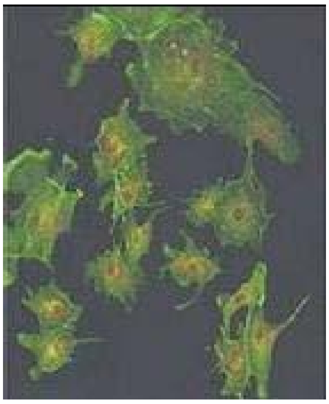


Figure 1.8 : Copy-Move Forgery/ Cloning: One of the recent famous cases of digital image forgeries in science - South Korean scientist Hwang Woo-suk claimed that he cloned stem cells

CHAPTER 2
LITERATURE REVIEW

Alin C. Popescu and Hany Farid [17] employ Principal Component Analysis (PCA) to small fixed size image blocks to yield a reduced dimension representation. This representation is robust to minor variations in the image due to additive noise or lossy compression. Duplicated regions are then detected by lexicographically sorting all of the image blocks. Detection is possible even in the presence of significant amounts of corrupting noise.

A.C. Gallagher [19], in an effort to detect interpolation in digitally zoomed images has found that linear and cubic interpolated signals introduce periodicity in variance function of their second order derivative. This periodicity is investigated by computing the Discrete Fourier Transform (DFT) of an averaged signal obtained fromthe second derivative of the investigated signal.

Weiqi Luo, Jiwu Huang and Guoping Qiu [20] compute seven characteristic features for each overlapping block - c_1, c_2, c_3 as the average of red, green, and blue components respectively. In the Y channel (Y=0.299R+0.587G+0.114B), a block is divided into 2 equal parts in 4 directions and compute c_4, c_5, c_6 and c_7 according to the formula c_i=sum(part(1))/sum(part(1)+part(2)) where i=4,5,6,7. For each block B_i, a block characteristics vector V(i) =(c_1(i),c_2(i),c_3(i),c_4(i),c_5(i),c_6(i),c_7(i)) is computed and saved in an array A. Then the array A is lexicographically sorted and similar block pairs are searched using some thresholds. This technique has lower computational complexity and is claimed to be more robust against stronger attacks and various types of after-copying manipulations, such as lossy compressing, noise contamination, blurring and a combination of these operations.

Babak Mahdian and Stanislav Saic [21] use blur moment invariants representation of the overlapping blocks. Blur moment invariants are suitable to represent image regions due to the fact that they are not affected by the blur degradation present in the region. Another advantage is that they are computed by a summation over the whole image, so they are not significantly affected by additive zero-mean noise. For determining similar blocks instead of lexicographic sorting, k-d tree representation is used. Like other existing methods, this method also has problem with uniform areas in images. Since identical or similar areas in the image are being searched, the method will logically label not duplicated parts also as duplicated in uniform areas, such as the sky. Thus, a human interpretation of the output of any duplication image regions detection method is obviously necessary. Another disadvantage of this method is its computational time.

A. Mahdian and S. Saic [22] have analyzed specific periodic properties present in the covariance structure of interpolated signals and their derivatives. Furthermore, an application of Taylor series to the interpolated signals showing hidden periodic patterns of interpolation is introduced. They also propose a method capable of easily detecting traces of scaling, rotation, skewing transformations and any of their arbitrary combinations. The method works locally and is based on a derivative operator and radon transformation.

Matthias Kirchner [23] gives an analytical description about how the resampling process influences the appearance of periodic artifacts in interpolated signals. Furthermore, this paper introduces a simplified resampling detector based on cumulative period grams.

S. Prasad and K. R. Ramakrishnan [24] have noticed that the second derivative of an interpolated signal produces detectable periodic properties. The periodicity is simply detected in the frequency domain by analyzing a binary signal obtained by zero crossings of the second derivative of the interpolated signal. When splicing is performed carefully, the border between the spliced regions can be visually imperceptible. In [25] and [26], the authors show that splicing disrupts higher-order Fourier statistics, which can subsequently be used to detect splicing. Photographs contain specific statistical properties. Some researchers have exploited the statistical regularities in natural images to detect various types of image manipulation [27, 28, 29]

M. K. Bashar et. al. [30] have proposed a wavelet based feature representation scheme for detecting duplicated regions in images. Multi-resolution wavelet decomposition is applied to small fixed-sized image blocks first. Normalized wavelet coefficients are then stacked in an order from lower to higher frequencies. This kind of representation appears robust to block matching. Duplicated regions are then detected by lexicographically sorting all of the image blocks and applying threshold tothe desired frequency of the offsets of the block coordinates. A semi-automatic technique that detects accurate number of duplicated regions is also proposed. Impressive results have been obtained compared to linear PCA based representation. The wavelet-based method has achieved higher precision with the comparable recall rates compared to PCA based method. However, the feature strength in the noisy and compressed domains has not been explored. To deal with the noisy environment the well-known algorithms for wavelet-based de-noising may be used. It may be necessary to integrate various characteristics of multiple wavelets or other information for more robust feature representation. Unlike other existing algorithms this algorithmworks even when the doctored image is truncated.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Preamble

One of the main purposes of image forgery is to conceal an object in the image. Normally the simplest way is to copy another portion of the same image and paste it over the object to be concealed such that it blends with the remaining part of the image and leaves no clues of tampering. To cover up any traces of forgery, retouching may be done at the periphery of the pasted object. An example of this kind is shown in figure 3.1.

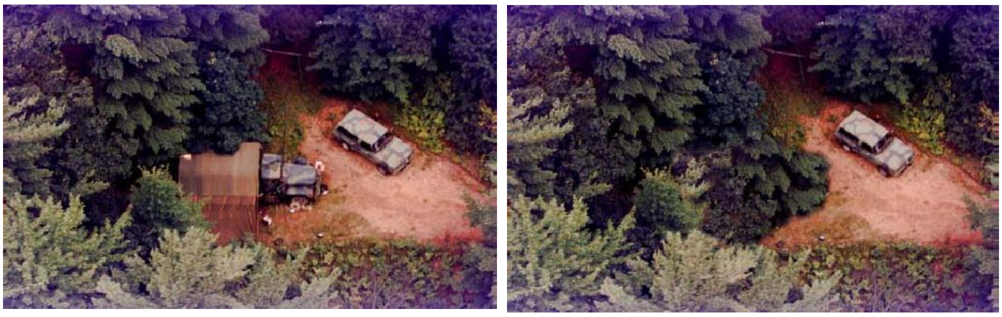


Figure 3.1: A truck in the original (left) is removed by covering with surroundingfoliage

The second purpose may be to replicate some object in an image. Then, a copy ofthe desired object in the image is made and pasted at one or more appropriate locations inthe image. Once again, to cover up any traces of forgery, retouching may be done at the periphery of the pasted object. An example of this kind is shown in figure 3.2.

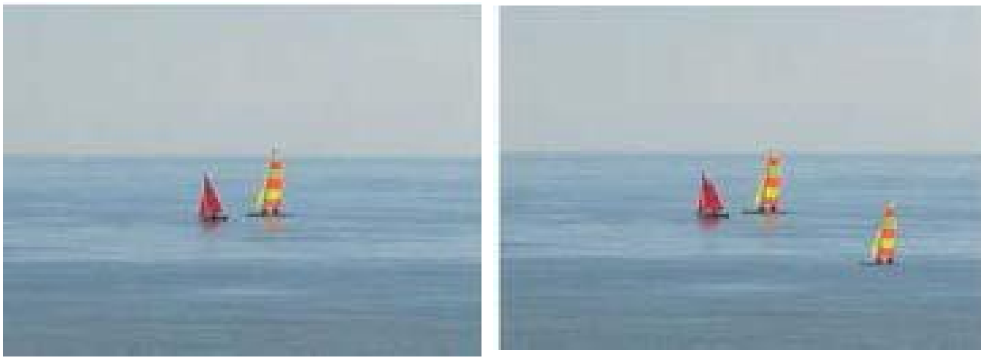


Figure 3.2: A boat with a yellow-orange hoist in the original (left) is replicated

There can also be a situation when an object from another image is copied and pasted at multiple locations in the forged image.

The Copy-Move forgery described above introduces a correlation between the original image object and the pasted one. This correlation can be used as a basis for a successful detection of this type of forgery. Because of the possibility of retouching and saving of the image in a loss compressed format like JPEG, the two objects may match only approximately and not exactly.

3.2 Exhaustive Search

The most obvious technique for detecting copied and pasted (duplicated) regions in the same image is to overlay the image and its circularly shifted version and search for closely matching image segments.

3.3 Block Match

A good method for detecting copy-move forgery is to verify if a set of blocks of pixels in a region of the image matches with another in a different region of the image. That is, the image is divided into *n* non-overlapping blocks, and each block is compared with the remaining ones. But, selecting the size of the block is difficult. If the size of the block is larger than the forged area, an exact match of the blocks does not result. If the size of block is smaller, the forged area may cross the boundaries of adjacent blocks and then also exact matches would not result. If the size of the block size is made very small, the matching process becomes computationally intensive, particularly with large images. Also uniform areas in the original image will be shownas duplicates. This kind of block matching can be termed as non-overlapped block matching.

3.4 Exact Match

A better alternative is to select overlapping blocks. Blocks of size bxb pixels are selected from the top-left corner, moving right and down, to the bottom-right corner one pixel at a time along the image. For each block the pixel values are extracted by columns into a row of a two-dimensional array A with (M–b+1) (N–b+1) rows and b^2 columns. Two identical rows in the matrix A correspond to two identical bxb blocks. To recognize the identical rows easily and quickly, the rows of the matrix A are lexicographically sorted. Matching rows can be easily searched by going through the rows of the ordered matrix A and looking for two successive rows that are identical.

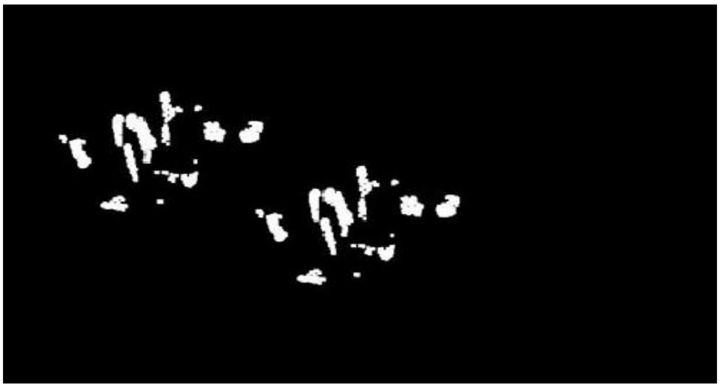


Figure 3.3: Copied and Pasted regions in the forged image 3.1

Discontinuities in the detected regions may be due to some retouching operation done after the forgery. But, if the forged image had been saved as JPEG, many of identical blocks would have disappeared because the match would become only approximate and not exact.

Figure 3.4 shows a forgery that could not be detected with a block size of 8x8 as retouching has been done after forgery. However, when the block size was reduced to 3x3, some blocks are shown as forged but many are false matches.

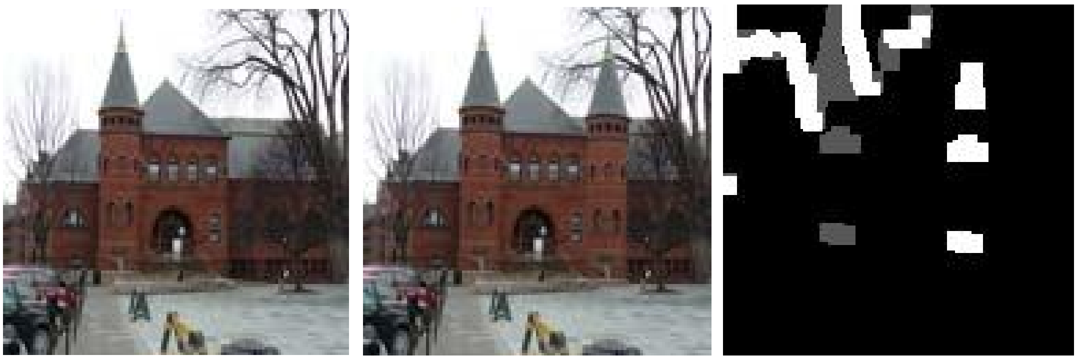


Figure 3.4 : Original Image (left), Forged Image (middle), and result of ExactMatch Algorithm with a block size of 3x3

It is observed that the Exact Match algorithm can detect plain Copy-Move forgeries but produces many false matches in retouched forgeries.

3.5 Robust Match

The best alternative to detect copy-move forgery is Robust Match where instead of matching the pixel representation of blocks, their robust representations are matched. One of the robust representations is the quantized DCT (Discrete Cosine Transform) coefficients. The advantage of DCT is that the signal energy would be concentrated on the first few coefficients, while most other coefficients are negligibly small. Therefore, the changes in high frequencies, which would occur due to the operations such as noise addition, compression, and retouching, do not affect these first coefficients greatly.

3.8 Modified Robust Match Technique

This method is same as the method discussed in section 3.6 in which quantizedcoefficients of DCT of blocks are used as block features. Here the length of the feature of the blocks is reduced which reduces the execution time without affecting the quality of the result. Reduction in the length of the feature sector is possible, because, when the quantization of DCT coefficients of the blocks is done, there are many long run zeros. These are high frequency DCT coefficients [78], which do not contribute to the quality of the image and hence can be omitted. The quantized DCT coefficients are read in zigzag order, as shown in Figure 3.10 and only quantized low frequency coefficients are taken.

3 .9 Performance Measures

The performance evaluation of a forgery detection algorithm can be done at two levels: at image level, where the focus is on the ability to detect if there is a forgery and at pixel level, where the accuracy of detecting the tampered regions [81]. In this work only image level evaluation is done.

Method	T_P	F_P	F_N	Precision	Recall	Score
Exact Match	50	0	100	100.00	33.33	49.62
Robust Match	110	20	40	84.61	73.33	78.56
Modified Robust Match	110	20	40	84.61	73.33	78.56

Table 3.1: Performance of the Block Matching forgery detection algorithms

CHAPTER 4

PROBLEM FORMULATION

4.1 Problem Background

In this day and age, digital images tampering has been made easy with widely available image editing softwares, such as Adobe Photoshop. The advancement of image editing softwares has reached a level such that image tampering can be done without degrading its quality or leaving obvious traces. This is alarming as images are now being presented as supported evidences and historical records in various fields, such as in forensic investigation, law enforcement, journalistic photography and medical images.

Moreover, in many instances tampered images have appeared in the news or social media, such as the manipulated images of Iranian missile test released on the 9th of July 2008 by Sepah News, the official media arm of Iran's Revolutionary Guard. The tampered image, shown in Figure 1.1 is aimed at exaggerating the country's military capabilities. The tampered image made its way into media circulation, making the front page of notable newspapers, such as The Financial Times and The Los Angeles Times. The forgery is detected a day later when the same source released another image taken from the same angle at almost the same time, but with different content.

The scientific community is also not spared from image tampering. Farid et al. stated that 20% of accepted manuscripts of the Journal of Cell Biology contains inappropriate figure manipulation. Hence, image tampering and detection have garnered substantial attention as manipulated images can be used to misrepresent their meaning with malicious intent.

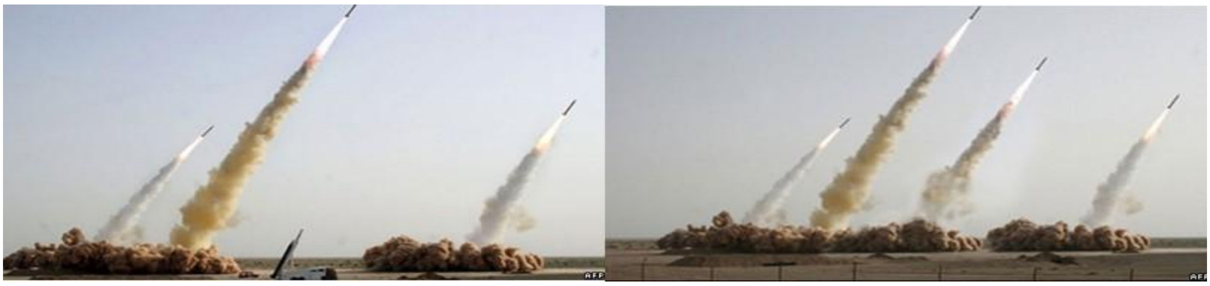


Figure 4.1: (a) Original image of Iranian Missile Test (b) Forged image of Iranian Missile Test

Among the image manipulation techniques in the literature, Abd Warif et al. stated that copy-move forgery and copy-move forgery detection (CMFD) is one of the most widely studied field. In general, CMFD involves the manipulation of an image where an object, texture or letter is copied from one region of an image and inserted into another region of the same image.

4.2 Problem Statement

The project focuses on applying widely used key point-based algorithms in the field of object recognition for CMFD. The proposed CMFD technique, consisting of both feature extraction and feature matching, would serve as an alternative to the current state of the art CMFD method using Speeded Up Robust Features (SURF).

Before SURF was introduced in the field of CMFD, Scale-invariant Feature Transform (SIFT) is widely regarded as one of the best key point-based algorithms for CMFD. With SURF, the algorithm proposed multiple optimization which successfully reduced the computation time by 3 times. However, the improvement came at the expense of the accuracy rate.

Hence, this work aims to identify a Copy Move Forgery Detection technique, consisting of both feature extraction (descriptor) and feature matching, capable of obtaining better accuracy rate while maintaining the computational time seen with SURF.

CHAPTER 5
RESULTS AND DISCUSSION

This chapter presents the experimental results of the copy move forgery detection algorithms presented in this thesis. All the three algorithms are first evaluated for their ability to detect simple copy move forgery. Then the algorithms are tested for detection ability of forged regions when additional manipulations are made to the copied image region before it is pasted. Dataset details are given in section 5.1 and the values assigned to the various pre-defined parameters required by the algorithms are listed in section 5.2. Section 5.3 briefs on the performance metrics employed and the further sections present the performance details of the proposed algorithms compared with existing algorithms.

5.1 DATA SET DETAILS

Dataset used for image copy-move forgery detection algorithms includes images manually created using Photoshop and also images from two bench mark datasets. The dataset contains 150 images of which 50 images werecreated using Photoshop and 100 images were collected from various sources. The two benchmark datasets used are “Database for object and concept recognition.

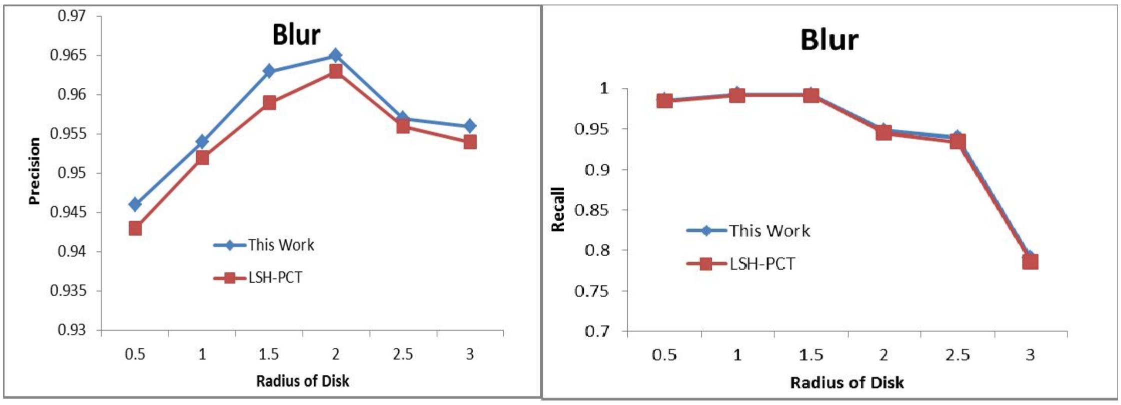
5.2 PERFORMANCE METRICS

Performances of the proposed copy move forgery detection algorithms are evaluated based on precision, recall and F1 score. Precision, recall and F1 score are metrics that reflect on the accuracy of detection. Precision and recall depend on three parameters namely number of images correctly detected as forged, number of images that are falsely detected as forged and the number of

- Robustness to rotational changes
- Robustness to additive noise
- Robustness to blurring
- Robustness to effects of JPEG compression

5.2.1 Robustness to Blur

Figure 5.1 shows the values of metrics with effect to the varying radii of blur filter applied to the images. The figure shows the Precision Recall& F1 score values of SH-PCT (mentioned as „this work‟), compared with existing PCT and Locality Sensitive Hashing (LSH - PCT) when blur filter of varying radius is applied.



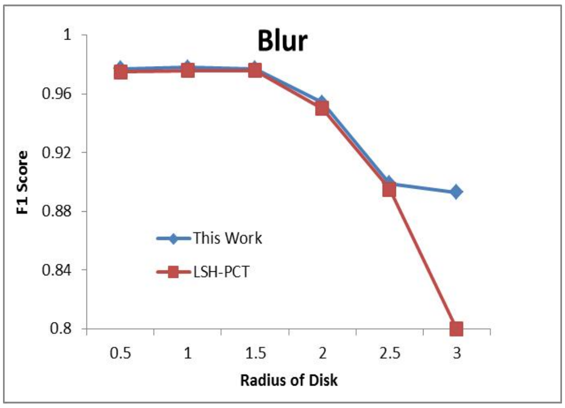


Figure 5.1 Comparison Of SH-PCT & PCT-Locality Sensitive Hashing (LSH - PCT) Algorithms' Performance in terms of Robustness To Blurring

5.2.2 Robustness to Noise

Figure 5.2 shows the values of precision, recall and F1 score plotted against noise of different levels of variance. The algorithm's performance compared with that of existing LSH –PCT method in detecting copy move forged images subjected to additional noise is recorded in the figure.

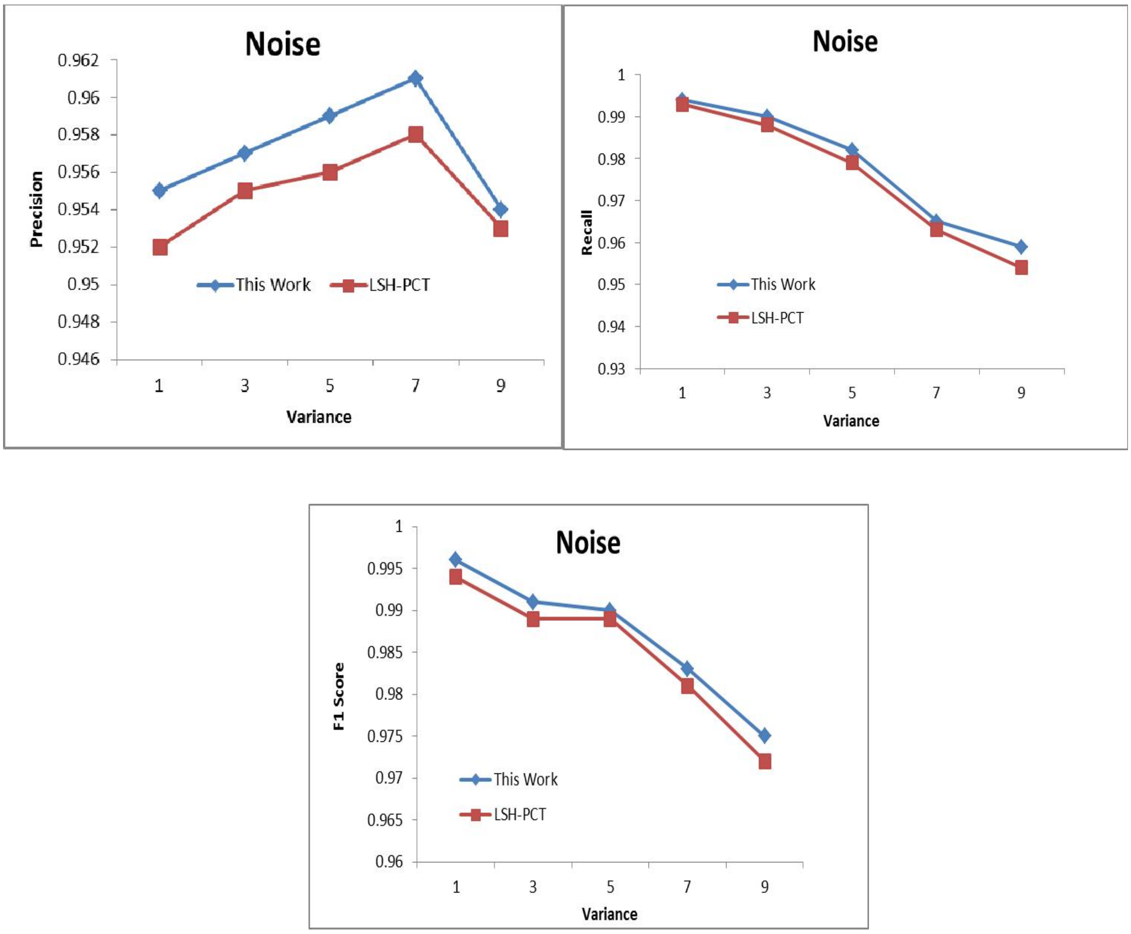


Figure 5.2 Comparison of SH-PCT & PCT-Locality Sensitive Hashing (LSH - PCT) Algorithms' Performance in Terms of Robustness to Additive Noise.

5.2.3 Robustness to the Effects of JPEG compression

SH-PCT algorithm is capable of detecting tampered regions effectively even when the images are compressed. To show this experimentally, forged images are compressed with varying quality factorsand then are used as inputs to the algorithm. Figure 5.3 shows the effects of the image being compressed with varying quality factors on the detection performance in terms of precision recall and F1 score. The graph shows the Precision Recall & F1 score values of SH-PCT (mentioned as „this work‟), compared with existing LSH - PCT CMFD algorithm when image undergoesJPEG compression of different quality factors.

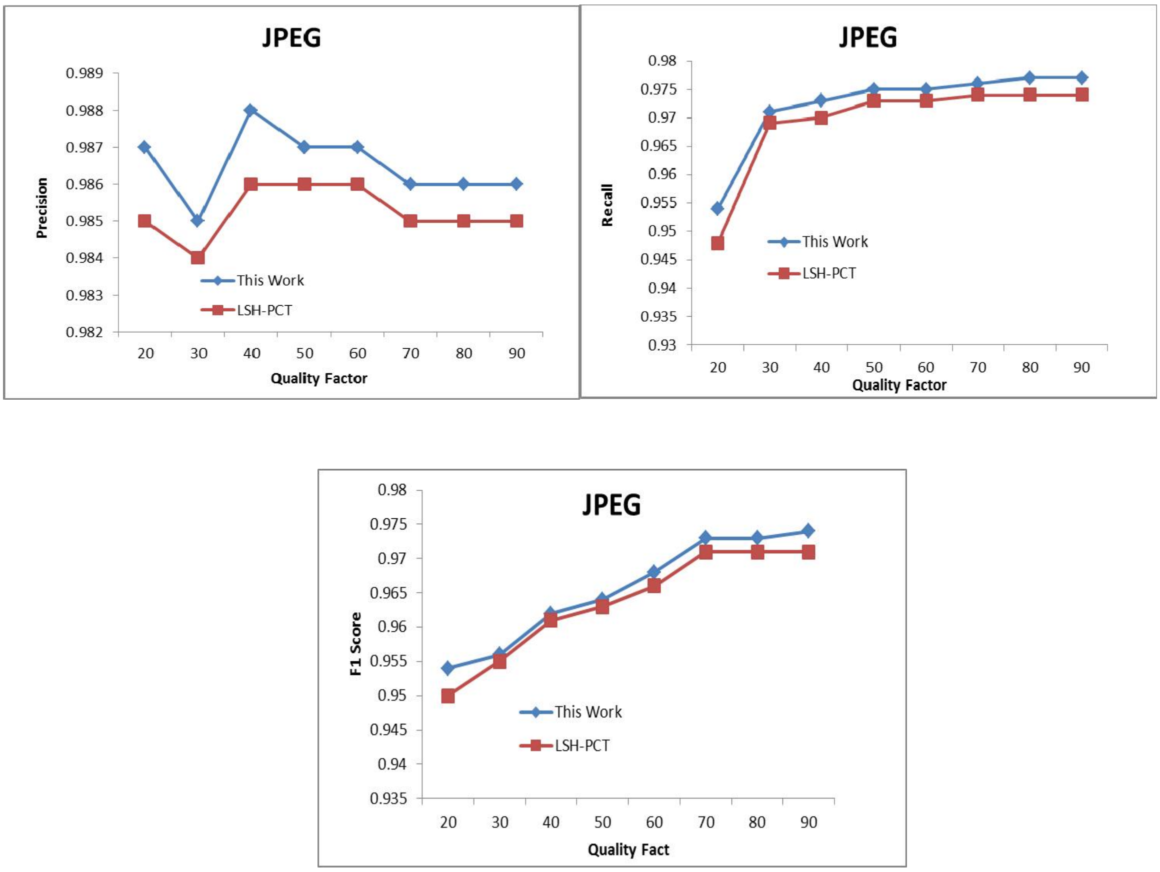


Figure 5.3 Comparison of SH-PCT & PCT-Locality Sensitive Hashing (LSH - PCT) Algorithms’ Performance with Respect to the Effects of Compression

5.2.4 Robustness to Rotational Changes

To show the algorithm’s ability to handle rotational changes made to the copied image portions copy rotate move forgeries involving different degrees of rotation are introduced in some of the images in thedataset and then were used in testing. The precision recall and F1 score values of the algorithms obtained when the copied region is rotated at different degrees and then pasted is shown in Figure 5.4. The figure also includes theperformance values of the existing LSH – PCT method.

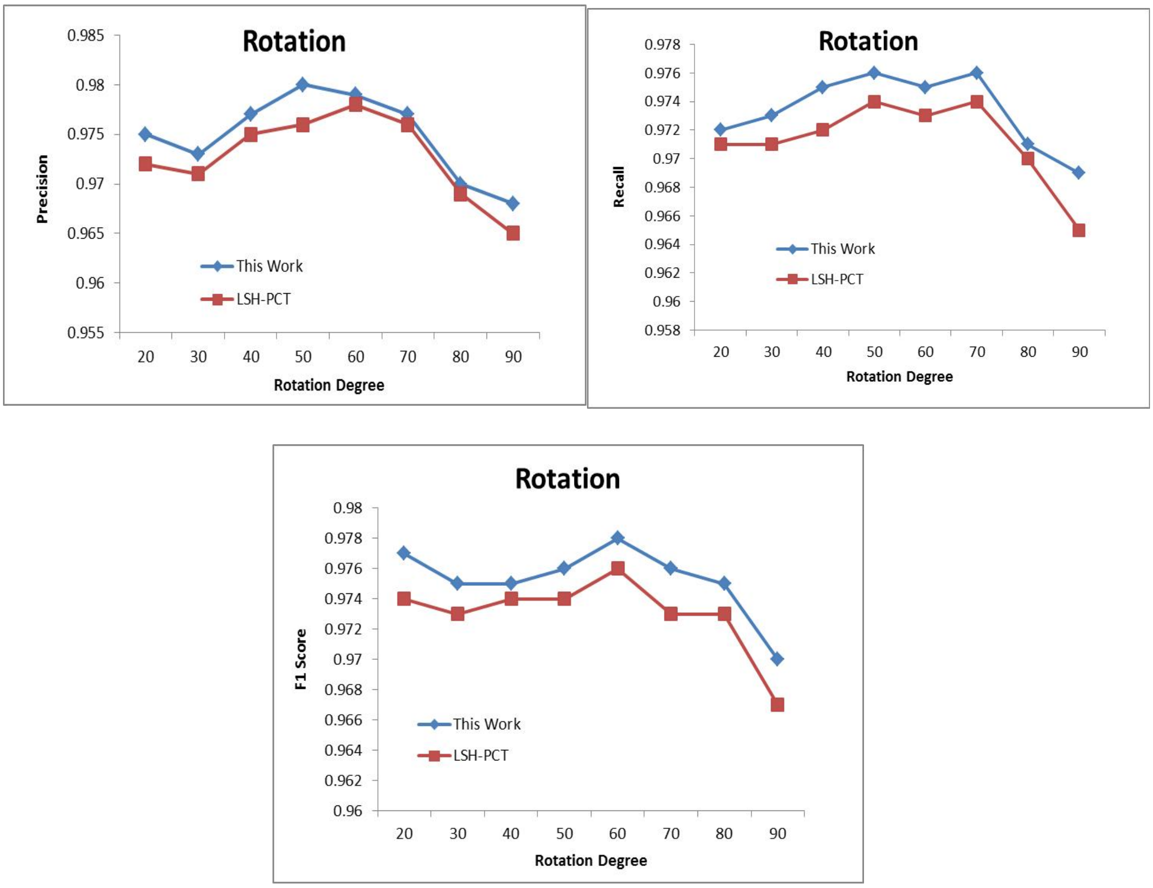


Figure 5.4 Comparison of SH-PCT & PCT-Locality Sensitive Hashing (LSH - PCT) Algorithms' Performance with respect to rotational changes.

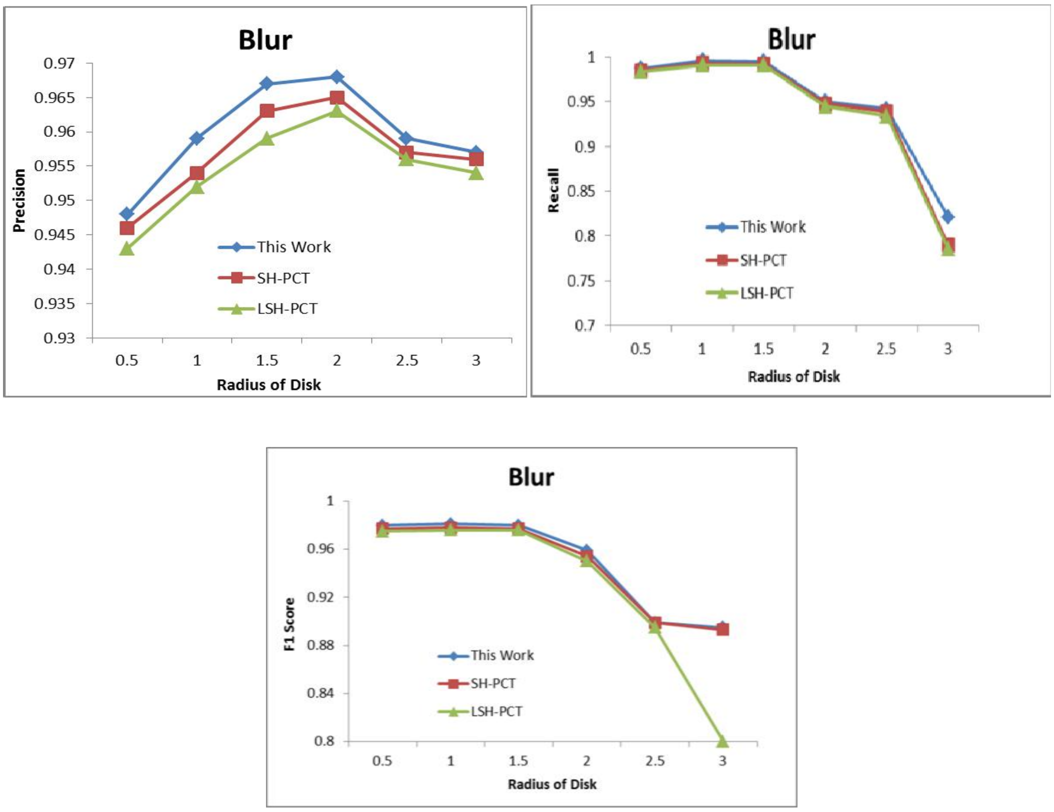


Figure 5.5 Comparison of MDSH-PCT with SH – PCT & LSH – PCTAlgorithms' Performance in terms of Robustness To Blurring

5.3 PERFORMANCE OF LEGENDRE MOMENTS & SHBASED CMFD ALGORITHM

The algorithm's detection accuracy of simple copy move forgery in terms of precision, recall and F1 score compared with that of existing Zernike moment-based region duplication algorithm is recorded in Table 5.3. The graphs in Figures 5.9 through 5.12 include the performance comparison ofthe Spectral Hashing Based Legendre moment algorithm (SHBLM) and an existing CMFD algorithm based on Zernike moments in cases of additional manipulations.

Method	Precision	Recall	F1 Score
Zernike Moments	0.92	1	0.96
Legendre Moments & SH	0.95	1	0.97

Table 5.3 Performance measures of Legendre moments & SH basedmethod compared with existing Zernike moment-based algorithm

5.3.1 Robustness to Blur

Figure 5.9 shows the values of metrics with effect to the varyingradii of blur filter applied to the images.

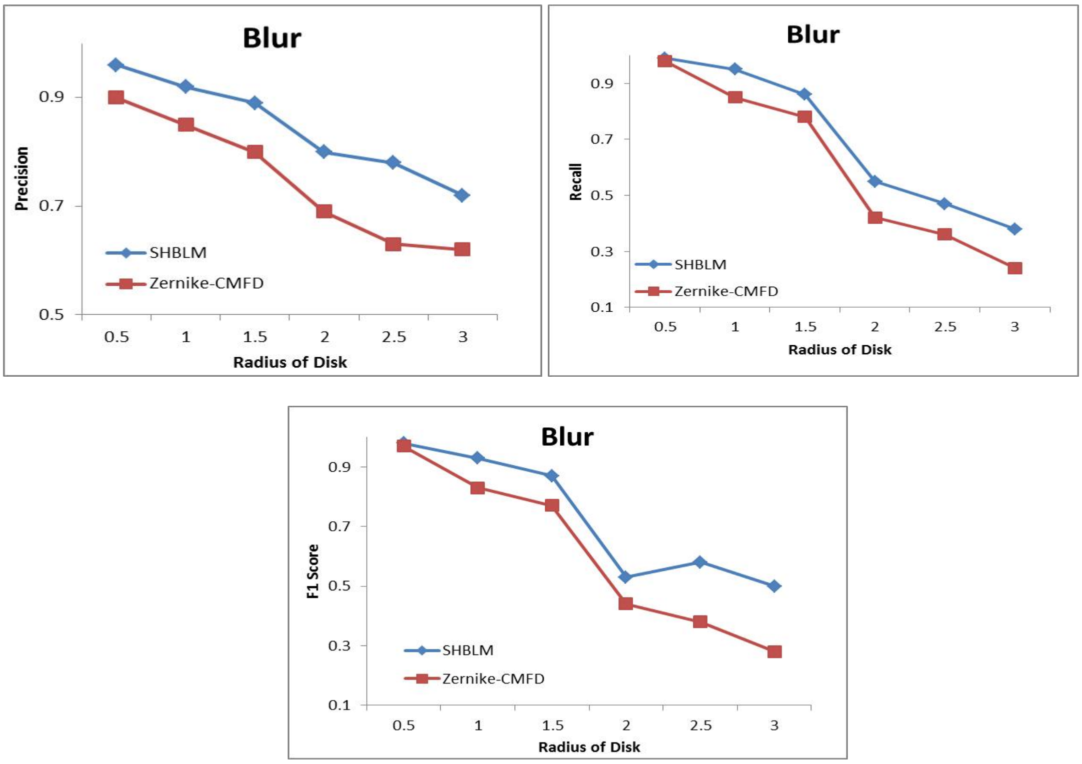


Figure 5.9 Comparison of Legendre moment based CMFD (SHBLM)and Zernike moment based CMFD Algorithms' Performance in terms of Robustness To Blurring

CHAPTER 6
CONCLUSION AND FUTURE AVENUES

Conclusion

Tampering images is not new. Availability of digital image technology and image processing software makes it easy for anyone to create a forgery. Not surprisingly, tampered images and videos are showing up everywhere, from courtrooms to scientific journals, and these images can have a profound effect on society. There is a clear need for tools to detect forgeries, and the field of digital image forensics has emerged to address this problem without any pre-requirements.

Five techniques for detecting different forms of tampering in manipulated digital images have been presented - Exact Block Matching Method and Robust BlockMatching Method, JPEG Compression Analysis Method and Geometry Based Method. Detection of forgeries in digital video - Frame Duplication and Region Duplication detection have also been presented.

Future Avenues

Image forensics is a burgeoning research field and despite the limitations of existing methods, promises a significant improvement in forgery detection. It has made and will continue to make it harder and more time-consuming to create a forgery that cannot be detected. Today’s technology allows digital media to be altered and manipulated in ways that were simply impossible 20 years ago. Tomorrow’s technology will almost certainly allow us to manipulate digital media in ways that today seem unimaginable. As new techniques for exposing photographic frauds are developed, newer techniques will be developed to make better fakes that are harder to detect. While some of the forensic tools may be easier to fool than others, some tools will be difficult for the average user to circumvent.

REFERENCES

[1] Tran Van Lanh, Kai-Sen Chong, Sabu Emmanuel and Mohan S. Kankanhalli, A Survey on Digital Camera Image Forensic Methods, IEEE International Conference on Multimedia and Expo, Beijing, China, pages 16-19, 2007.

[2] "Photo Tampering Throughout History", http://www.fourandsix.com/

[3] Tehseen Shahid, Atif Bin Mansoor, Copy-Move Forgery Detection Algorithm for Digital Images and a New Accuracy Metric, International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009, pp 159-161.

[4] www.verifeyed.com

[5] Alessandro Piva, An Overview on Image Forensics, Hindawi Publishing Corporation ISRN Signal Processing Volume 2013, Article ID 496701.

[6] Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato, Detecting Forgery From Static-Scene Video Based onInconsistency in Noise Level Functions, IEEE Transactions On Information Forensics and Security, Vol. 5, No. 4, December 2010, pp.883-892.

[7] Christian Rey, Jean-Luc Dugelay, A Survey of Watermarking Algorithms for Image Authentication, EURASIP Journal on Applied Signal Processing, Hindawi Publishing Corporation 2002:6, 613–621.

[8] Babak Mahdian, Stanislav Saic, A Bibliography on Blind Methods for Identifying Image Forgery, Signal Processing: Image Communication 25, pp. 389–399, Elsivier.

[9] Hany Farid, Image Forgery Detection - A Survey, IEEE Signal Processing Magazine, Vol. 2, No.26, 2009, pp. 16–25.

[10] Jessica Fridrich, David Soukal, and Jan Lukas, Detection of Copy-Move Forgery in Digital Images, Proceedings of Digital Forensic ResearchWorkshop, IEEE Computer Society, Cleveland, OH, USA, August 2003, pp. 55–61.

[11] Zhang W., Cao X., Zhang J., Zhu J. & Wang P., Detecting Photographic Composites Using Shadows, Proc. IEEE International Conference on Multimedia and Expo ICME 2009, pp. 1042-1045.

[12] Mo Chen, Jessica Fridrich, Miroslav Goljan, and Jan Lukas, Determining Image Origin and Integrity Using Sensor Noise, IEEE Transactions on Information Forensics and Security, 2008, Vol. 3(1), pp. 74-90.

[13] Davide Cozzolino, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva, Springer-Verlag Berlin Heidelberg, SSPR & SPR 2012, LNCS 7626, 2012, pp. 693–700.

[14] LUO Weiqi, QU Zhenhua, PAN Feng, HUANG Jiwu, A Survey of Passive Technology for Digital Image Forensics, Frontiers of Computer Science in China, 2007, 2(1): pp. 1−11.

[15] Osamah M. Al-Qershi, Bee Ee Khoo, Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art, Forensic Science International 231 (2013) 284–295.