Forensic Analysis of Cloned Regions of Digital Images using Feature based methods

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE

OF

MASTER OF TECHNOLOGY

IN

SIGNAL PROCESSING AND DIGITAL DESIGN

Submitted by:

VAISHALI KIKAN

2K17/SPD/19

Under the supervision of

DR. N. JAYANTHI

DEPARTMENT OF ELECTRONICS AND COMMUNICATION

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

JUNE,2019

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I Vaishali Kikan, 2k17/spd/19 student of M.Tech Signal Processing and Digital Design, hereby declare that the project Dissertation titled "Forensic Analysis of Cloned Regions of Digital Images using Feature based methods" which is submitted by me to the Department of Electronics and Communication Engineering, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology/Bachelor of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi **VAISHALI KIKAN**

Date:

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled "Forensic Analysis of Cloned Regions of Digital Images using Feature based methods" which is submitted by Vaishali Kikan, 2k17/spd/19 [Department of Electronics and Communication], Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology/Bachelor of Technology, is a record of the project work carried out by the students under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

Date:

DR. N JAYANTHI

Assistant Professor

Department of Electronics and communication Delhi Technological University, Delhi

SUPERVISOR

ACKNOWLEDGEMENT

I thank GOD almighty for guiding me throughout the semester. I would like to thank all those who have contributed to the completion of my project and helped me with valuable suggestions for improvement.

I am extremely grateful to Dr. N. Jayanthi, Division of Electronics and Communication, for providing me with best facilities and atmosphere for the creative work guidance and encouragement.

Above all I would like to thank my parents without whose blessings; I would not have been able to accomplish my goal.

……..

VAISHALI KIKAN

ABSTRACT

Digital technologies have gained immense attention of the researchers recently due to extensive use of digital techniques in everyday life. Our government has also started programs like Digital India, which has also enhanced the use of Digital media and mostly Digital images in everyday life and thus its use in forensics has also increased tremendously. Digital images are quite simple to tamper because advanced image processing and editing tools are easily available today. Today, adding or removing important features from an image without leaving any visible mark that the image has been tampered is very easy, which is a serious social issue as well as it is used by criminals to alter the important features of the image so that they can escape punishments easily. As information processing in digital domain is replacing analog processors and the digital image and video cameras replacing analog ones, the requirement to authenticate the digital images to legitimize their content, and detecting copy move forgery is only increasing. In this thesis, a special type of widely used image tampering method i.e. cloning, in which a single or multiple portions of an image are copied and then they are moved somewhere else in the same image and pasted there with the motive to hide any important detail of the image or to replicate the given feature many times in the image of interest. Image forgery is the technique of detecting image modification, either with the previous information about the source image (active) or without (passive). Further the images can be scaled, rotated, shifted or flipped, thus detection of the forgery in the image is further made difficult. In comparison to the earlier studies, our thesis gives a better representation as well as comparison, challenges and future work in a well organized manner.

In this thesis, we study a new feature based technique which when combined with clustering, SWT, RANSAC will provides us better results. Following techniques are used to detect the cloned image and localization of the cloned areas of the image which describe the thesis in a nutshell.

Cloning detection is a block based technique which use extensive search to detect the cloned portions of the image. There are 2 block based search algorithms that can be used in this technique, which are Exact Match and Robust Match. Exhaustive search is done after computing the autocorrelation of the given image and then it is ready for application of various feature based and non feature based techniques which are described below:

- DCT based technique: In this a sliding window of 16X16 dimension is used to compute the DCT matrix of the image whose coefficients are quantized and inserted in a row which is lexicographically sorted. Rows that match exactly will give the location of the cloned portions of the image.

- SIFT based technique: In this SWT is computed to preprocess the image then SIFT is computed on the approximate sub band produced during SWT. The 4 steps used to calculate SIFT and then key points are extracted and then matching and clustering of the extracted key points is done and at last RANSAC is used to remove false positives in this image. This technique will also provide the cloned regions but is better than DCT because it can be used for rotated rescaled clones.

- MIFT based technique: In this SWT is computed to preprocess the image same like we did in SIFT to compute the approximate sub band. The 4 steps used to calculate MIFT which generates quality vectors with the help of their neighborhood and then descriptor is formed and then matching and clustering of the extracted key points is done and at last RANSAC is used to remove false positives in this image. This technique will also provide the cloned regions but is better than DCT because it can be used for rotated rescaled clones.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS, ABBREVIATION

CMFD : Copy Move Forgery Detection

SIFT : Scale Invariant Feature Transform

MIFT : Mirror Reflection Invariant Feature Transform

DCT : Discrete Cosine Transform

SWT : Stationary Wavelet Transform

RANSAC : Ranom Sample Consensus

TP : True Positive

TN : True Negative

FP : False Positive

FN: False Negative

TPR : True Positive Rate

FPR : False Positive Rate

CHAPTER 1 INTRODUCTION

In recent years, broad research has been led to detect the copy move picture forgery or cloning in digital images because of various advancements in the digital technology. The simple accessibility of cutting edge image processing and editing softwares makes it simple to remove any important part of the digital picture or add any critical part from one or numerous digital pictures, without leaving any visible mark that the given picture has been manipulated. Digital manipulation can be of any kind and these sorts ca n likewise be improved. In light of this Genuinity of pictures can't be determined by just looking the image. The kind of picture forgery is classified into 3 frames. This is done based on cloning system.

Image retouching is considered as the least destructive kind of digital image manipulation, which does not fundamentally change a picture but rather upgrade or obscure certain highlights of this picture, thus help in enhancing the contrast, sharpness and brightness of the image. It is very well known among magazine photograph editors and even every individual has done this sooner or later of time to improve certain highlights of our picture with the goal that it will turn out to be more appealing, overlooking the fact that these manipulations are morally wrong. Fig.1.1 demonstrates the digital images before and after applying image retouching technique on it.

Fig 1.1 After and before applying image retouching technique

Cloning is identified with Splicing whereas in this case, just a single picture is utilized for producing the forged image rather than two images. In cloning, some portion of a picture is copied and the consistency can be kept up with the help of blurring the edges of the cloned region Fig. 1.2 demonstrates a case of cloning. In the final image one of the pencils is hidden with the help of background area. The background grey area is selected from the image and a piece of this background is used to hide the pencil by placing this portion of the background exactly over the desired pencil. In different cases, the copied portion of a manipulated picture can be rotated, scaled, flipped and can even be retouched before cloning the given image with this segment of image. Thus this technique to manipulate image is very dangerous in forensics as many important parts of the image can be hidden with the help of this technique and also the number of any important detail can be enhanced any number of times. For example, instead of hiding the given pencil in fig 1.2, the number of pencils can be increased by copying a pencil and placing it on background or above other pencils. Thus this technique is really dangerous for forensic studies where the criminal may hide an important portion of the image.

Fig 1.2 Cloning or copy move image forgery to remove one pencil

Among these techniques, we will concentrate on Copy-Move image forgery or cloning. Another case of cloning is appeared in fig.1.3, in which the paper pattern demonstrates 3 distinct photos were utilized in making the final picture. The 1.3 images are: Image of White House, Image of Bill Clinton and Image of Saddam Hussain. In this, the image of White House was blurred and rescaled to make a deception of an out of center

background. Now at that point, Bill Clinton and Saddam Hussain were cut off from their separate distinctive pictures and kept on the primary background to make a meaningful final image. The right shadow and lightning were safeguarded and the speak standing with microphone was deliberately acquired so this is a case of the extremely practical looking image cloning .

INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

1 2 3

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Fig 1.3 splicing of 3 different images to form forged image

The following case of digital image cloning was given in the general conference by Dr. Tomaso A. Poggio at Electronic Imaging 2003 in Santa Clara. In his discussion, he showed that the lip movement of any individual, while he is talking, can be learned by specialists and afterward the lips were digitally manipulated to arbitrarily change the spoken words. For instance, a video cut demonstrating a TV anchor who was broadcasting the news was forged to make him look like he is singing a well known melody rather, while maintaining the match between the tune and lip movement. This reality that individuals can utilize digital softwares to carefully tempering pictures and video to make unrealistic and arbitrary circumstances threatens to limit the reliability of videos and pictures appeared as proof in forensic analysis without realizing the fact that the video and images are in advanced manipulated form with the help of tempering

softwares. One can easily digitize the simple analog video clip, transfer it into software, perform the required frauds, and afterward save the generated output forged video in the NTSC design on a customary tape. The circumstance will additionally deteriorate as the software that perform imitations will get leaked from research labs and come out in the real world as a business tool

The necessity for discovery of advanced digital frauds has been recognized by researchers, yet at present new research work and papers publication is generally less. Delicate content validation, content confirmation, identification of manipulation, localization of alterations, and recuperation of real images and videos are done through digital watermarking. While digital watermarks can give essential data about the picture integrity and we know it's preparing history that the watermark must be available in the picture before the tempering of the content. Thus its application is restricted to constrained conditions that incorporate military frameworks or surveillance cameras. Tempering in the-wild will be perceivable utilizing a watermark just when all advanced obtaining gadgets are furnished with a watermarking chip. It may happen, yet to utilize inadvertent camera "fingerprints" identified with the noise of the sensor; its shading array, as well as its dynamic range to find the manipulated regions in pictures is extremely troublesome. Classifying surfaces that are present in characteristic pictures utilizing statistical means and discovering inconsistencies in those statistics between various segments of the picture is another strategy for blind forgery discovery. Such methodologies will give huge number of missed location and additionally false positives.

Fig 1.4 Watermarking of image to protect it from tempering

MOTIVATION

Picture forensics is largely utilized these days for detecting criminal. It is required in view of the popularity of picture and video fraud, which began in mid 1840s. The individual behind the deceitful picture was H. Bayradwas, he was pictured like he was about to commit a suicide.

Next tempered picture came out in 1860s¸in which the face of A. Lincoln was cloned over J. Calhoun. The scenes which are graphical splicing are extremely common in Hollywood movies in which Computer graphic softwares assumes a critical position.

Forged photographs additionally assume critical position in war publicity, where these are used mostly to inculcate hatred among masses. Different recordings of Osama Bin Laden came into picture in the tragic episode of 9/11 which, after further examination, were identified to be tempered. Fig 1.6 shows the tempered pictures of Osama Bin Laden shown by Pakistani news channel and was also published in British Newspaper Mail, Times, Telegraph, Sun & Mirror.

Today different instruments are accessible by which the advanced pictures can be adroitly and effortlessly tempered. In light of this foreseeing the Genuinity of photograph has turned out to be very troublesome.

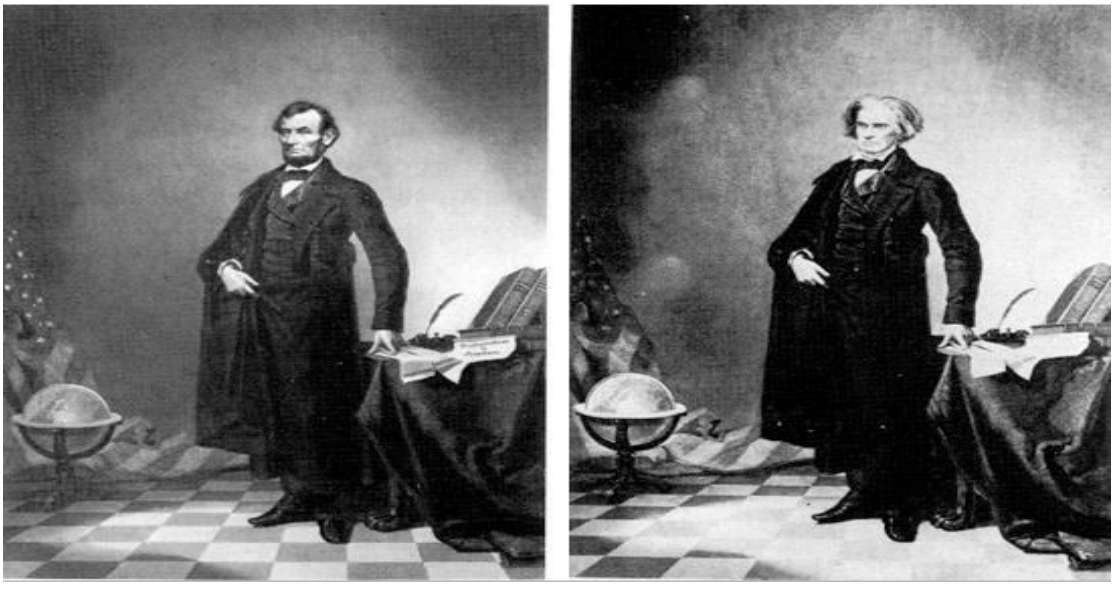


Fig 1.5 The face of A. Lincoln was cloned over that of J. Calhoun with the help of copy move technique

Thus we saw the trend of image forgery was started in 19th century and after that it has increased on a rapid scale. We know that the pictures speak louder than the words and this phrase is actually true as the images contain significantly larger information than the equal amount of words. Pictures can speak more than a witness can, but the advancedsoftwares that are tempering these images are a real drawback to the criminal identification system of our forensic labs.

To detect the authenticity of the images produced as witnesses, we need advanced tools so that the real justice can be guaranteed and criminals may not escape the punishment with the use of advanced digital cloning tools to modify the witness images for their advantages.

Many algorithms have been developed for the final development of an advanced digital software which would easily detect the tempering with greater efficiency, accuracy and in lesser time. This work is another such algorithm which provides faster and accurate results.

Fig 1.6 Tempered picture of Osama Bin Laden published by British Newspaper Mail, Times,Telegraph, Sun & Mirror and also broadcasted by Pakistani news channel

APPLICATIONS

The uses of image cloning detection approaches are as per the following:

- Forensic examination in labs
- Criminal examination as a witness of crime in courts
- Insurance handling and digital pension schemes where a person has to submit a proof that he is living or died in order to avail benefits.
- Surveillance frameworks in various government departments which required additional safety like atomic energy, foreign procurement, foreign relations and other departments like RBI and also private companies which requires great piece of safety.
- Intelligence administrations for the safety of the nation from terrorists and criminals and from bank or other robbery also.
- Medical imaging for the diagnosing of various fatal diseases at a early stage.
- Journalism for prevention of spreading the false information or misleading the people of the nation

It will be useful in finding the truth of a picture. Further uses are to indicate whether the popularity demonstrated is unique, as number of individuals can be expanded or diminished through cloning techniques. It is very essential to discover the manipulation when somebody or something is covered up in a picture.

EVOLUTION OF IMAGE FORGERY DETECTION TECHNIQUES

As of late, many image cloning detection algorithms and tools have been produced and have reviewed and in this study I have discovered that a portion of these strategies can be combined for cloning recognition and better efficiency with the help of feature based

methods like SIFT(scale invariant feature transformation) and reflexive SIFT. The methodologies to detect cloning are characterized into two classes:

- Active approach (Non Blind) and
- Passive methodology (Blind)

Active cloning recognition strategies requires the previous data about the real picture and for this the access to the original image is required which is quite difficult in real time applications, for example, a reference format or various kinds of features extracted from the original image. Thus they are not programmed. These methods have restricted applications in light of the fact that the genuine picture is inaccessible in generally in every handy situation.

Passive techniques are the most recent strategies and have more extensive application since they don't require anything from the developer. Thus the original image is not required and hence this technique has made many new researchers to work for it.

Our newly devised algorithm is a further extension of the passive technique in which we are not provided with the original images and only forged images are available. Thus the features of only forged images are enough for the detection and localization of the cloned areas of the images. Fig 1.7 shows the manipulated image in the left in which George Bush is holding the upside down book whereas in the original image he is holding the book in the correct way.

Fig 1.7 The forged image in the left shows George Bush holding the book upside down and its original image at the right.

Fig 1.8 shows the forged image of leaders in white house in left and its real image in right.

Fig 1.8 The forged image in the left shows George Bush holding the book upside down and its original image at the right.

Various active techniques are given below:

- Watermarking
- Greenspan et al.
- Onishi and Suzuki
- Choi and Kim In Xiong and Quek
- Ulas et al.

Various passive techniques are given below:

- Pixel-dependent
- Format- dependent
- Camera- dependent
- Physics- dependent
- Geometric- dependent
- Using Expectation Maximization (EM)
- Rescaling Detection Method

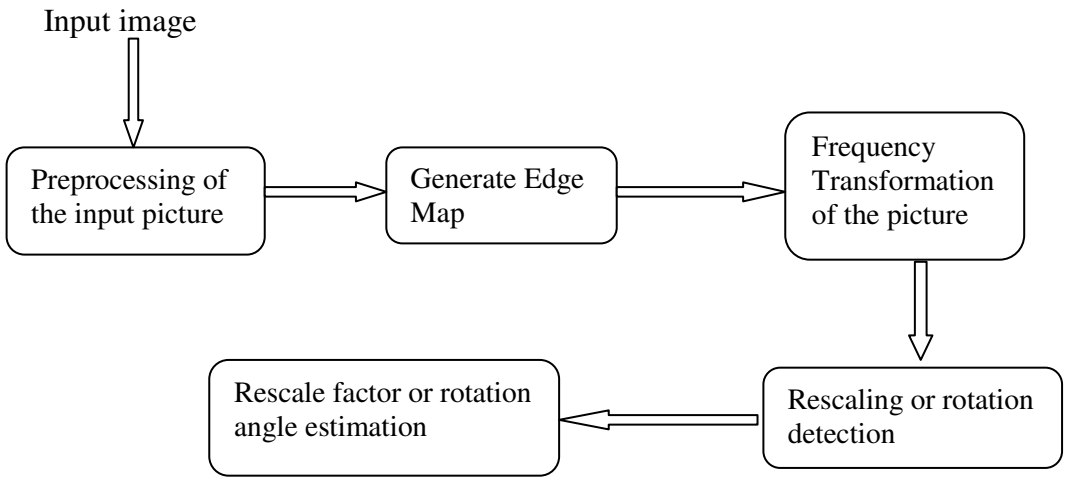


Fig 1.9 Flow diagram of Re-sampling detection technique

- Contrast enhancement (Intrinsic Fingerprinting)

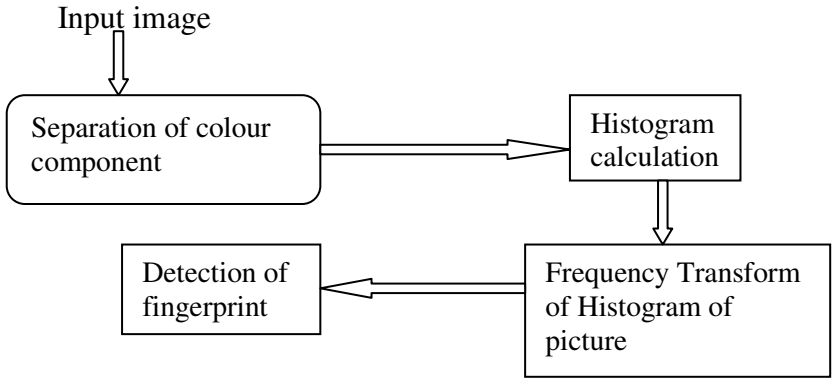


Fig 1.10 Flow diagram of Contrast enhancement detection technique

SUMMARY

The above mentioned methodologies have various preferences as they can manage a wide range of geometric changes, blurring and disfigurement. The space and time required for count is likewise less as compared with square based techniques. Yet at the same time there are following issues.

- These approaches are not suitable for flat areas of the image.
- High false positive rate (FPR) of the recognized outcome.

- Accurate method for cloning localization isn't accessible.
- Computational efficiency is relatively less.

CHAPTER 2 CLONING

COPY MOVE FORGERY

In light of the extraordinary work of the issue and its exceedingly unexplored structure, the categorizing forgeries by their mechanism and analyzing every forgery type contrastingly is the basic necessity. In attempting that, an assorted Forensic Tool Set will be constructed. Despite the fact that every software may not be powerful enough to give adequate proof that the provided image is digitally forged, when the full combination of devices is utilized, a researcher can join the combined proof and effectively give the best answer. The initial move towards creating the FTS is taken by remembering one extremely broad class of tempering, the digital Copy-Move forgery, and making proficient algorithms for its accurate location.

In a Copy-Move modification, a piece of the picture is cloned into another piece of a similar picture to influence a question "to vanish" from the picture by covering it with the replicated segment. Finished territories like grass, foliage, rock, or texture with uneven pattern, are perfect for this reason in light of the fact that the duplicated zones will effortlessly mix with the given background and the human eye can only with significant effort distinguish it.

Since the cloned portion was taken from the same picture, its component of noise, color pattern, dynamic range, and other essential attributes will be in correlation with whatever is left on the picture and subsequently won't be recognizable utilizing calculations that search for contrasting qualities in statistical measures in different fragments of the picture. To improve the cloning, one can utilize the feathered cropping or the correct retouching to additionally hide any hints of the cloned portions.

Instances of the Copy-Move falsification are shown in Fig 2.1, in which, a truck was covered with the help of cloning of foliage.

Fig 2.1 Forged picture is above where jeep is hidden with the help of cloning, downside is real picture

DETECTION OF CLONING

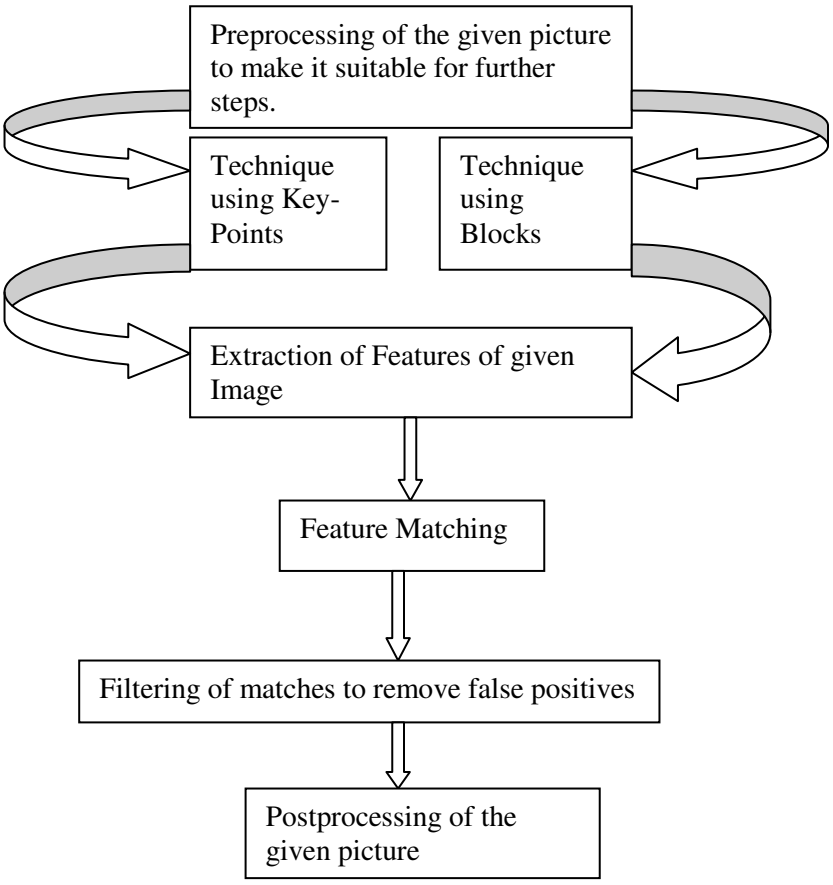
In cloning detection, there is comparability between the genuine picture and the replicated section of the fake image. This correlation between different sections of the image can be utilized for the identification of this sort of modification, as the change will presumably be saved at some location in the lossy JPEG design and the utilization of the retouching tools or diverse localized image modification algorithms, the fragments will just roughly correlate not completely. Henceforth, we can locate the accompanying necessities for the detection algorithm:

- The recognition algorithm or the detection tool ought to give an inexact and inappropriate matching or correlation of the picture segments.

- Less computational time for detecting the image is forged or not and also for the detection of the exact place where cloning is performed on the image i.e. localization of cloning.

- False positives should be detected and localized in the image so that unwanted complications don't arise in the detection of cloning.

- The cloned portion will be a connected fragment instead of an accumulation of contracted patches or couple of pixels.



2.2 Flow diagram image cloning detection tecnique

The process for identification and localization of cloned regions is given below :

EXHAUSTIVE SEARCH

This is the direct and most conspicuous strategy. In this methodology, the picture and its circularly shifted duplicate or modified image are confronted searching for exceptionally

correlating picture fragments.

Envision that x_{ij} is the pixel estimation of a grayscale picture of size L×M at the position (i, j). The accompanying contrasting values are recorded:

$$|x_{ij}\text{-}x_{i+k}\text{mod(L).(j+l).mod(M)}|, \quad \ldots 1$$

Where;

k= 0,1,……L-1;

n= 0,1,……M-1 for all i and j.

On comparing x_{ij} and its cyclical shift [k,n] is equivalent to contrasting x_{ij} and its cyclical shift [k',n'], where k'=L– k and n'=M– n. Consequently, it satisfactory to identify just those movements [k,n] with $1 \leq k \leq L/2$, $1 \leq n \leq M/2$. Hence the complexity of computation was cut by a factor of 4. For every shift [k,n], the distinctions Δx_{ij} are figured and thresholded with a very small limit t but the determination of the threshold limit is complicated, in light of the fact that in normal pictures, the pairs of the pixel will provide contrasts underneath the given threshold t but we are just interested on associated fragments of certain negligible size.

Henceforth, the thresholded contrast Δx_{ij} is then modified utilizing the morphological opening function in which, the image is first eroded and after that dilated with the neighboring pixels comparing to the insignificant size of the duplicated territory. The opening function expels isolated points. Despite the fact that this technique is powerful yet is computationally expensive too. In this manner, due to exhaustive search, it is illogical for medium and large sized pictures.

Amid the identification, all of the shifts [k,n] with $1 \leq k, l \leq L/2$ should be distinguished. For every shift, every pixel pair would be taken into consideration, compared, thresholded, and afterward the entire picture must be dilated and eroded. The correlation and picture manipulation require the order of LM tasks per move.

Therefore, the aggregate computational requirements are corresponding to $(LM)^2$. For instance, the computational prerequisites for a picture that is twice as large are 16 times bigger. Consequently it is utilized for only small pictures as it were.

AUTOCORRELATION

The computation of autocorrelation of the picture x of the size L×M is given below:

$$r_{k,n} = \sum_{i=1}^{L} \sum_{J=1}^{M} x_{i,j}\ x_{i+k,j+n} \quad ...2$$

Where,

i,k = 0,1,…..,L-1,

j,n = 0,1,……,M-1,

The autocorrelation can be effectively and easily computed using the Fourier transform:

$$r = x * \hat{x}, \quad ...3$$

Where,

$\hat{x} = x_{L+1,M+1-j}$,

Where,

i = 0,1,…..,L-1,

j = 0,1,……,M-1,

Thus,

$$r = F^{-1}\{F(x).F(\hat{x})\}, \quad ...4$$

The autocorrelation between the real and replicated fragments will provide peaks in the autocorrelation for the movements that will relate to the cloned fragments of the same image. Be that as it may, on the grounds that natural pictures contain their power distribution in the low-frequency area in most of the cases. If the autocorrelation (r) is

determined for the picture itself then very large peaks will be present at the corners and their neighborhoods. In this way, we register the autocorrelation from its high-pass filtered adaptation of the given image so that false positives will get removed. A few high-pass filters were attempted like :

- Marr edge detector
- Laplacian edge detector
- Sobel edge detector
- Noise extraction utilizing the 3×3 Wiener filter.

Here we found out that the best one was the 3×3 Marr filter.

Let the insignificant size of a cloned fragment is B, the autocorrelation clone location technique comprises of the accompanying methodologies:

1. First take the test image and apply the Marr high pass filter.
2. Figure out the values of autocorrelation r of the picture obtained after step 1.
3. As the autocorrelation is symmetric, we can remove half of them.
4. Now we are left with only 2 corners and we have to set r = 0 in these two corners.
5. Locate the value of r where it is maxima and then distinguish the shift vector and now look at the shift utilizing the exhaustive technique (this technique is currently computationally proficient in light of the fact that we don't need to play out the exhaustive search operation for a wide range of shift vectors).
6. On the off chance that the recognized segment is bigger than B, stop here, else perform the operation in Step 5 with the following maxima of r.

In spite of the fact that, this strategy does not have an expansive computational complexity, it regularly neglects to identify the fraud except of the case when the size of the cloned zone is minimum $\frac{1}{4}$ of the linear measurements of the image. Both of these strategies were relinquished for the third technique that worked essentially better and quicker over these methods.

The third technique being the block matching technique which is significantly better and thus helped us achieve better true positive rate and lesser false positive rate

DETECTION OF CLONING WITH BLOCK MATCHING TECHNIQUE

- Exact Match

This technique is for distinguishing those fragments in the picture that are precisely matched. Despite the fact that the relevance of this algorithm is restricted, it might at present be helpful for scientific investigation of the images related to the crime. It additionally frames the premise of the robust match that will be presented in the following section of the given image.

To start with, the client indicates the small size of the portion that ought to be utilized for match. Give us a chance to assume that this portion is a square with A×A pixels. We will slide the square by one pixel along the picture from the upper left corner right and down towards the lower right corner. For each segment of the A×A window, the pixel magnitude from the window of this block are extracted by sections into a 2D array of a two-dimensional cluster B with A^2 segments and (L– A+1)(M– A+1) row. Each line compares to one position of the sliding square.

Fig2.3 Result obtained out of cloning detection Block matching technique in the exact match mode when the Block size(A) is taken to be 1

Two indistinguishable rows in the matrix B relate to two indistinguishable A×A clones. To recognize the indistinguishable rows, the rows of the matrix B are lexicographically arranged. This should be performed in L.Mlog(L.M) steps. The rows which are matched exactly are effortlessly searched by going through all L.M rows of the arranged matrix B and searching for two back to back rows that are exactly same.

Fig 2.3 shows the matching blocks that are found in the BMP picture of Jeep of Fig 2.11 for A=8. The blocks frame an unpredictable example that nearly coordinates with the cloned foliage of the given image. The way that the blocks frames a few disengaged pieces rather than one associated fragment shows that the individual who did the cloning of the image has most likely utilized a modify device like blurring on the cloned section to cover the hints of the forgery. Note that if the manipulated picture had been saved as JPEG, greater part of indistinguishable blocks would have vanished on the grounds that the match would turn out to be just rough and not correct.

- Robust Match

The thought for the robust match recognition is like the correct match with the exception that we don't need to do the organization and match the pixel representation of the blocks yet their robust portrayal that comprises of quantized DCT coefficients. The quantization steps are determined from a client indicated parameter Q. This parameter is equal to the quality factor in JPEG compression, i.e., the Q factor decides the quantization steps for DCT change coefficients. Since higher estimations of the Q-factor lead to better quantization, the squares must match all the more intently so as to be recognized as comparative. Lower estimations of the Q-factor create all the more coordinating squares and thus will create potentially some false matches.

The recognition starts similarly as in the exact match case. The picture is checked from the upper left corner to the lower right corner while sliding a A×A square window. For each square window, the DCT transform is determined; the DCT coefficients are quantized and put away as one row in the matrix B. The network will have (L– A+1)(M–

A+1) lines and A×A sections concerning with the correct match case. The rows of B are lexicographically arranged as previously. The rest of the method, be that as it may, is unique. Since quantized estimations of DCT coefficients for each block are presently being looked at rather than the pixel portrayal, the calculation may discover too many matching clocks that are false matches.

In this way, the calculation additionally takes a look at the common position of each coordinating block combine and yields a particular block pair just if there are numerous other coordinating pairs in the equivalent shared position i.e. they have a similar move vector. Towards this objective, if two back to back rows of the arranged matrix B are discovered, the calculation stores the places of the coordinating blocks in a different list. For instance, the coordinates of the upper left pixel of the block will be taken as its position and increases a shift vector counter C.

Let the position of the coordinating blocks be (i_1, i_2) and (j_1, j_2). The shift vector 's' between the two coordinating blocks is determined as

$$s = (s_1, s_2) = (i_1 - j_1, i_2 - j_2). \quad ...5$$

Since the move vectors – s and s relate to a similar shift, the shift vectors s are standardized, if fundamental, by multiplying by – 1 so that $s1 \geq 0$.

For every coordinating pair of blocks, we increase the standardized move vector counter C by one:

$$C(s_1, s_2) = C(s_1, s_2) + 1 . \quad ...6$$

The shift vectors are determined and the counter C augmented for each pair of back to back coordinating rows in the arranged matrix B. The shift vector C is instated to zero preceding the calculation begins. Towards the finish of the coordinating procedure, the

counter C shows the frequencies with which distinctive standardized shift vectors happen. At that point the calculation will discover all normalized shift vectors.

s (1), s (2), …….. , s (K) , whose event surpasses a client determined edge T: C(s (r)) > T for all r = 1, ……. , K. For all standardized shift vectors, the coordinating blocks that added to that explicit shift vector are hued with a similar color and hence recognized as sections that may have been cloned.

The estimation of the limit T is identified with the size of the littlest fragment that can be recognized by the calculation. Bigger values may make the calculation miss some not really firmly coordinating blocks, while too little an estimation of T may present an excessive number of false matches. We rehash that the Q factor controls the sensitivity of the calculation to the level of coordinating between blocks, while the square size A and limit T control the insignificant size of the section that can be identified.

For the robust match, we have chosen to utilize a bigger size of block, A=16, to forestall an excessive number of false matches as we know that the bigger blocks have bigger fluctuation in DCT coefficients. Nonetheless, this bigger block size implies that a 16×16 quantization lattice must be utilized rather than basically utilizing the standard quantization matrix of JPEG. We have discovered from extensive research that all AC DCT coefficients for 16×16 block are on average considered 2.5 times bigger than for 8×8 blocks and the DC expression is twice as large. In this manner, the quantization matrix (for the Q-factor Q) that is utilized for quantizing the DCT coefficients in each 16×16 block has the following structure

$$Q_{16} = \begin{pmatrix} Q'_8 & 2.5q_{18}I \\ 2.5q_{81}I & 2.5q_{88}I \end{pmatrix} \quad \ldots 7$$

Where,

$$Q'_8 = \begin{bmatrix} 2q_{oo} & \cdots & 2.5q_{18} \\ \vdots & \ddots & \vdots \\ 2.5q_{81} & \cdots & 2.5q_{88} \end{bmatrix}$$

also, Q_{ij} is the standard JPEG quantization matrix with quality factor Q and I is a 8×8 unit matrix (all components equivalent to 1).

We recognize that this frame is fairly specially appointed, but since the matrix gave great execution in pragmatic tests and in light of the fact that little changes to the matrix impact the outcomes practically nothing, we didn't examine the determination of the quantization matrix further.

Note in regards to the colored pictures:
In both Exact and Robust Match, if the dissected picture is a color picture, it is first changed over to a grayscale picture utilizing the standard formula:

$$I = 0.299\ R + 0.587\ G + 0.114\ B, \qquad \ldots 8$$

before continuing with further investigation.

RE- SAMPLING DETECTION METHOD

We used the method described in Gallagher (2005) and Wei et al. (2010) for detecting re-sampling in digital images. The steps in the method for detecting re-sampling consists of five steps:

(1) Pre-processing
(2) Edge map generation
(3) Frequency transformation
(4) Detection of rotation/rescaling
(5) Estimation of rotation angle/ rescaling factor.

- Pre-processing

The input image is first converted into the YCbCr color space. The motivation for choosing YCbCr color space is that it is perceptually uniform and is a better approximation of the color image processing. The luminance component that is the Y component alone is then separated from the YCbCr
color image.

- Edge map generation

A pattern of second order difference, i.e., the edge map of the input image is generated by convolving the luminance (Y) component of the input image with 3 X 3 Laplacian operator. Thus the remaining steps are done on the edge map of the input imag

- Frequency transformation

The one dimensional DFT is calculated for the edge map. There are two methods for calculating the DFT such as DA (DFT þ Averaging) and AD (Averaging þ DFT) methods.

In DA Method, the magnitude of DFT is calculated for each row of the edge map and then the average is taken over all the rows to get the horizontal spectrum.

Assume that E(m, n); mϵ[1,M]; nϵ [1,N] are the entries of the edge map and F is the Discrete Fourier Transform. The DA method can be expressed as follows:

$$E_{DA} = \frac{1}{M}\sum_{m-1}^{M} |F[\mathrm{E(m,\ n)}]| \qquad ...9$$

In AD Method, the average of all rows of the edge map is calculated to form a horizontal row and then the magnitude of DFT is calculated to get the horizontal frequency spectrum. The AD method can be defined as follows:

$$E_{DA} = F\{\frac{1}{M}\sum_{m-1}^{M} |E(m, n)|\} \quad ...10$$

- Detection of rotation/rescaling

The horizontal frequency spectra obtained from DA and AD methods are plotted separately against frequencies to form DA and AD curves respectively. Only half of the curve is considered because the DFA plot is symmetrical. Peaks appear in DA and AD curves because of maximum magnitude value in the frequency spectrum if the image is resampled. The appearance of peaks is due to interpolation.

When an image or image block is re-sampled, interpolation takes place in the re-sampled image or image block. The interpolated regions and their derivatives have inherent periodicity. Due to interpolation-induced periodicity, the frequency spectrum contains peaks directly related to the scaling factors (Remember in rotation also the image is rescaled with a scaling factor proportional to rotated angle). The frequencies of the peaks formed referred as peak frequency are used for estimating the rotation angle and rescale factor.

The reason for using two methods (DA and AD) is for distinguishing rotation and rescaling. Though rotation and rescaling behaves in a similar manner, they differ in certain cases which may be used for distinguishing them. Peaks formed due to rotation appear only in DA method and the peaks formed because of rescaling appear in both DA and AD methods.

- Estimation of rotated angle/rescale factor

The rotated angle/rescale factor can be estimated by using the peak frequency obtained from the DA and AD curves.
Rotation angle estimation formula is given as follows:

$f_{rot1} = 1 - \cos \Phi \; ; \; 0 < \Phi \leq 60$

$$\cos \Phi \; ; \; 60 < \Phi < 90 \qquad \ldots 11$$

and

$$f_{rot2} = \begin{cases} \sin\Phi \; ; \; 0 < \Phi \leq 30 \\ 1 - \sin\Phi \; ; \; 30 < \Phi < 90 \end{cases} \qquad \ldots 12$$

where Φ is the rotated angle and f_{rot1} , f_{rot2} are the peak frequencies induced due to rotation. The rescale factor estimation formula is given as follows:

$$f_{res} = \begin{cases} 1 - \frac{1}{R} \; ; \; 1 < R < 2 \\ \frac{1}{R} ; \; R > 2 \end{cases} \qquad \ldots 13$$

Or

$$f_{res} = \frac{1}{R} - 1 \; ; \; R < 1 \qquad \ldots 14$$

where R is the rescale factor and f_{res} is the peak frequency induced due to rescaling. The first equation is used when the image size is enlarged and the second equation is used when the image size is reduced. By substituting the obtained peak frequency from DA and AD curve in the above estimation formulae, Q or R can be calculated. The formation of rescale factor and rotation angle estimation formulae can be referred from Gallagher (2005) and Wei et al. (2010).

HISTOGRAM METHOD

In this method, a very simple and effective method is presented which uses the analysis of histograms of doubly compressed images and some features in the histogram are then utilized in order to differentiate the doubly compressed area from that of singly compressed area. The method is effective in the sense that it can detect

forged region accurately and at the same time, it is computationally more efficient as opposed to the previous techniques of forgery detection. It uses a feature based clustering on the grayscale version of the image which makes computationally efficient. It classifies the area of the image as original or tampered based on feature computed on the histogram of a doubly compressed JPEG image.

The subsections presented in this section first covers the study and analysis of how a histogram of doubly compressed image differs from that of singly compressed image and then a method to detect forgery is presented based on this analysis.

Analysis of Histogram

Here, the histograms of two types of images are analyzed; one is singly compressed, while the other is doubly compressed. The histogram of a singly compressed image is having smooth distribution of frequencies whereas the histogram of a doubly compressed image can be seen in one of two ways, first it contains high peaks and deep valleys if the second compression is of lower quality.

Second, the histogram contains periodic zeroes if the second compression is of higher quality. The above behaviour is also explained in [2].

The proposed method uses this analysis in order to detect double compression in the image and finally detect the forged regions in the image if exist.

The analysis shows that when a part of a non-compressed image is pasted onto a JPEG image and it is again compressed then the histogram of such an image is a mixture of two histograms, one containing smooth distribution and the other containing either periodic zeroes or containing high peaks and deep valleys which are actually a result of double compressed part in the image.

This is shown in Fig. 2.5

.

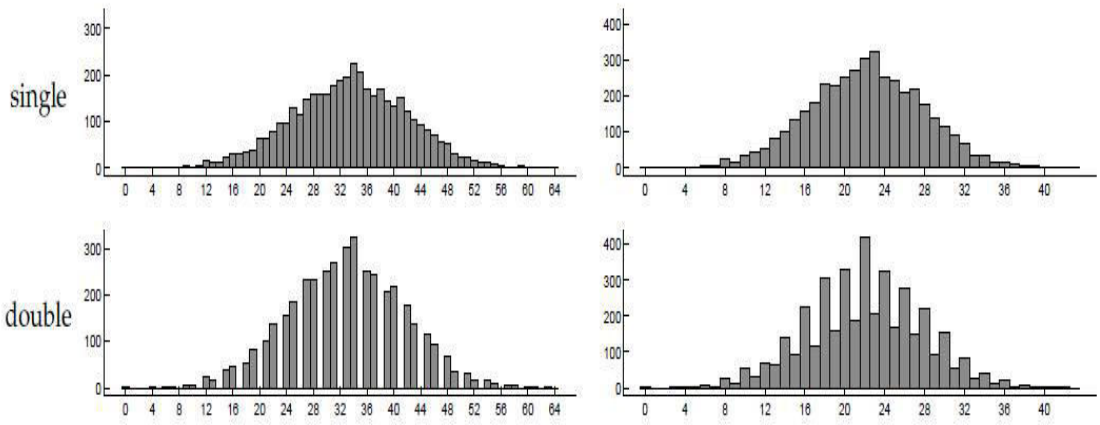


Fig 2.4 Histogram analysis of compressed and doubly compressed images

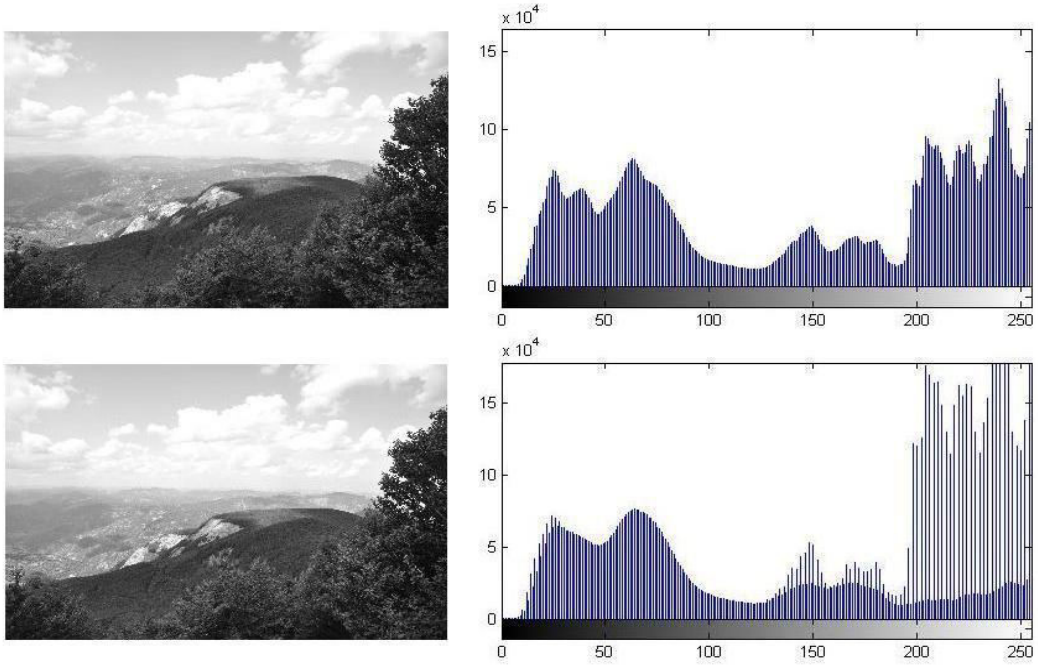


Fig 2.5 Histogram of original image and that obtained after the compressed image is pasted over non compressed image.

The analysis shows that the distribution of pixel frequencies contains a greater number of outliers if the image is doubly compressed whereas a singly compressed image contains a less number of outliers.

Therefore, we have chosen a feature 'kurtosis'[12] for finding whether the distribution is outlier prone or not. The greater value of kurtosis denotes a greater

number of outliers whereas a value less than or equal to 3 denote that the distribution does not contain outliers.

Forgery Detection

The above method for detecting double compression can be used in detecting forgery in the image. The same method for detecting double compression can be applied for finding out whether parts of image have undergone a single or double compression. For this, we can use the feature 'kurtosis'[12] for detecting the presence of single or double compression. Now, we divide the complete image into blocks of size 512x512 and then each block is tested for the presence of single or double compression. The parts which have undergone a double compression can be categorized in one cluster whereas the other parts which are only singly compressed can be categorized into another cluster. Therefore, the forged region which is just singly compressed can be declared as forged.

The algorithm consists of following steps:

1. Read an image.
2. Convert to a grayscale image.
3. Test an image whether parts of it have undergone double compression or not as proposed in A.
4. Divide the image into 512x512 blocks.
5. Obtain histogram of each block.
6. Calculate kurtosis on count of number of pixels in the histogram.
7. Construct a vector of these features and use them in a k-means classifier. Keep the value of k as 3.
8. Sort the clusters according to number of blocks in each cluster.
9. Choose the second cluster as a cluster containing suspicious blocks.

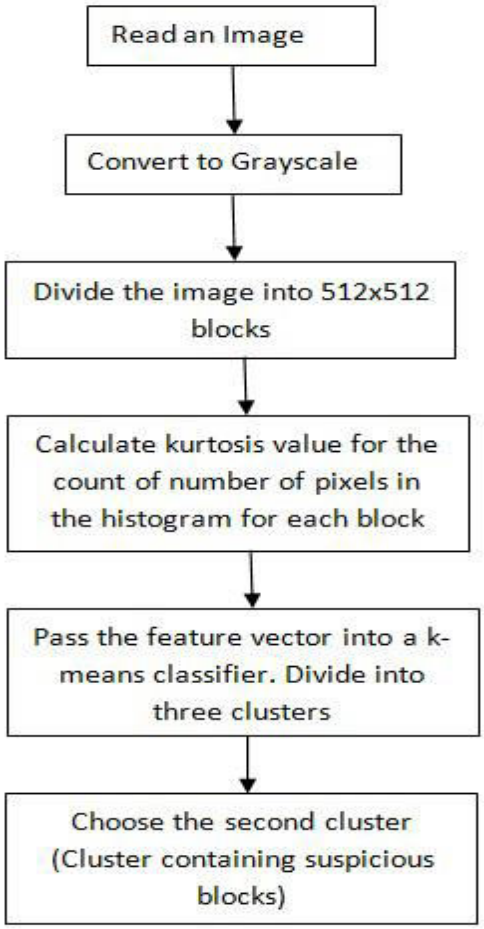


Fig 2.6 Method to detect image forgery with the help of cluster based technique

While performing copy-move forgery, the doctored/forged part in the image will form a lesser area in the image in comparison to undoctored/non-forged area. Therefore, the method assumes that the forged area in the image is smaller in comparison to the non-forged area in the image. The method divides the image blocks into three clusters; after dividing into three clusters, the clusters are sorted according to the number of blocks and then the second cluster is chosen as containing suspicious blocks. Ideally, blocks should be divided in only two clusters; the clusters containing forged and non-forged blocks. The cluster containing a lesser number of blocks can be declared as forged one.

But, the experimental results have shown that some of the blocks have a feature value which is much higher in comparison to the feature value of other blocks; to segregate those blocks having very high value of 'kurtosis', the blocks have been divided into three clusters; the first cluster in the sorted order is having those blocks, it contains very few blocks having exceptionally high values of kurtosis. The second cluster in the sorted order is now declared as forged. The third cluster contains larger number of blocks and is declared as nonforged. Upon analysis, it has been seen that a few blocks are having exceptionally high values because of the same color distribution in the histogram of that block. That means, that block contains a very high number of pixels at the same intensity in the grayscale version of the image because of which an exceptionally high value of kurtosis is generated. These values of kurtosis which are generated for a few blocks can be segregated as a cluster containing minimum number of blocks. The second cluster however, is designated as the cluster containing forged blocks.

DCT ALGORITHM

This algorithm can be broken into four steps.

- The first step is to compute the DCT of each 16X16 sliding window in the image.
- For each of these blocks, the coefficients of the DCT are quantized with an extended JPEG quantization matrix.
- After all of the blocks are quantized, they are inserted as rows into a matrix and then lexicographically sorted.
- Next, adjacent rows that match in the matrix are identified and for each match a shift vector is computed.

The shift vector is calculated as

$$s(i) = [x(1) - x(2), y(1) - y(2)] \quad \ldots 15$$

Where x(i)and y(i) are the coordinates of the blocks in the image that match.

For each s(i), a count tells the number of times it has been seen. For all s(i) that have a count greater than some user specified threshold, the blocks corresponding to that shift vector are colored in the original image as possible forged regions.

It is important to point out that the algorithm has two parameters that influence its effectiveness. The first input is a quality factor that weights the quantization matrix. The higher the quality factor, the more likely dissimilar blocks will be marked as matches. The lower the quality factor, the less likely it is to have false matches and a higher quality match is likely to be found. The other important parameter of Sheehan 3 the algorithm is the threshold mentioned before. This threshold determines the number of shift vectors that must be the same for a match to be marked as a forged region. A higher shift vector enforces a restriction that more blocks must be copied together for that region to marked as a forged region.

After implementing the algorithm described above in MATLAB, many false positives were identified regardless of the parameters chosen. After many tests, it was noticeable that a majority of the false positives were from shift vectors [1,0] , [0,1] , and [1,1]. Therefore, the algorithm was adjusted to not consider any of these three shift vectors as forged regions. The results of this slight variation are shown in section three and the effectiveness of this algorithm on regions with rotation and scaling is explained.

SIFT ALGORITHM

In SIFT and SURF i.e. feature based methodology key-point feature is extricated to frame key-point descriptor vector that afterwards is utilized to produce cluster for matching cloned segments. In HOG based methodology, 1-D DWT is utilized to get the approximate picture that is then further subdivided into smaller blocks and later every

such block is utilized to discover HOG features which are then correspondingly utilized for framing clusters for coordinating manipulated areas of the image. In previous section, we introduced a block based strategy to distinguish cloning forgery utilizing Discrete Cosine Transform (DCT) of the picture blocks. Initially, all of the blocks are sorted lexicographically and afterward the neighboring comparable pairs of the blocks are viewed as the clones. Restriction of this strategy is that it neglects to distinguish very small clones.

A technique utilizing Principal Component Analysis (PCA) is utilized. In this methodology, the picture is sectioned into a few blocks and after this, at that point their feature vectors are determined and arranged lexicographically. The advantage of this technique is that it can decrease time complexity and also works useful for extensively larger pictures. Yet, its accuracy diminishes for the small digitized blocks.

The identification strategy for cloning forgery detection dependent on SWT-SVD is likewise utilized for cloning forgery recognition. SWT technique is shift invariant as well as noise invariant which is utilized to disintegrate the picture presented by the user and aides in discovering similarity between various blocks of a picture. This model distinguishes cloning forgery for blurred picture fruitfully.

- Proposed model

The motivation behind proposed technique is to recognize cloning forgery in advanced pictures. To begin with, the picture provided by the user is decomposed with SWT which is later used to extricate key-point features by applying SIFT. Then these extricated features are utilized to frame clusters which help to discover coordination among various cloned segments of the image. To get the last aftereffect of the picture, the coordinating outliers are removed. The work process of our proposed model is appeared in Figure 2.7.

- Pre-processing

The preprocessing block of the flow diagram in Fig 2.7 includes two sub-steps:

Firstly, the info picture is changed over to grayscale on the case that it is a RBG picture. The purpose for changing over it into grayscale is to decrease multifaceted nature by changing over a 3D pixel magnitude (R, G, B) to a 1D magnitude.

Other than decreasing the complexity, we know that the color data does not contribute in distinguishing key-point features. The accompanying equation is utilized to change over the RGB magnitudes to grayscale magnitudes.

The second step being the use of SWT to get four sub groups, for example:

1. swa(approximate)
2. swv(vertical)
3. swd(diagonal)
4. swh(horizontal

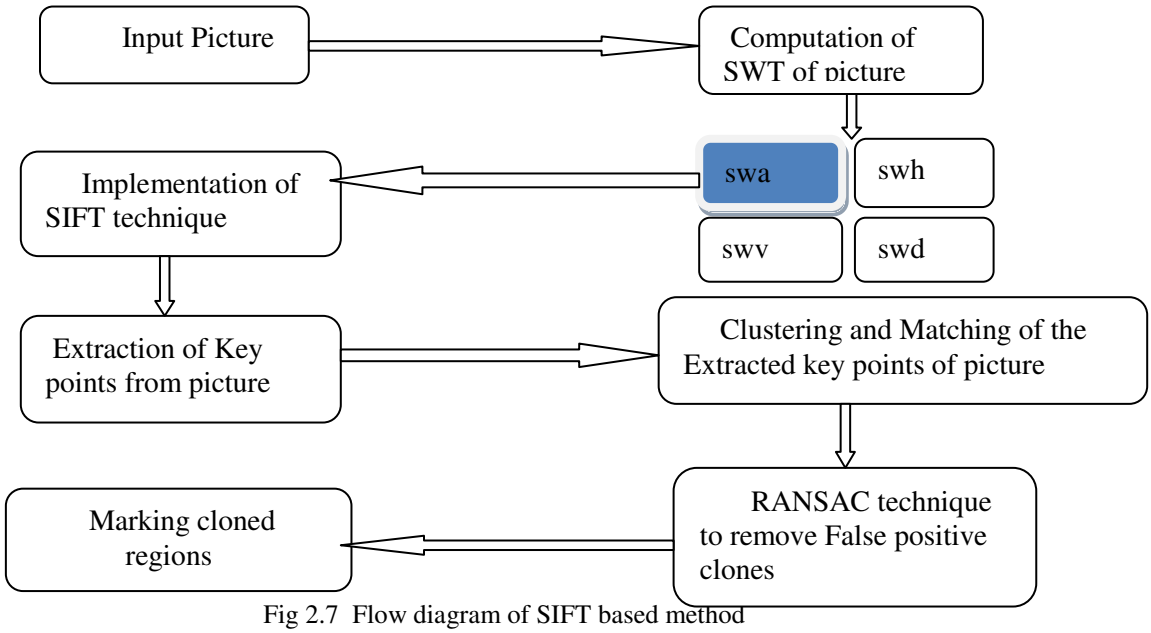


Fig 2.7 Flow diagram of SIFT based method

Fig 2.7 presents the flow diagram of SIFT based method to find out the cloned regions in the input image and Fig 2.8 represents the output image generated after decomposition by SWT on input image.

Fig 2.8 Demonstrates the image generated after decomposition by 2D-SWT on input image.

The image is decomposed into 4 segments in first level and in next level its swa sub-band is further divided.

- SIFT Feature Extraction

SIFT is extraordinary compared to other component separating calculation proposed by David Lowe. It is invariant to geometrical transformation, image rotation, change of viewpoint and change in intensity in matching the features of the image. The calculation is separated into 4 fundamental processes. They are as per the following:

1. Scale Space Extrema Detection

In this process Gaussian of Difference (DoG) is utilized to discover the points of interest (POI) which are invariant to scaling and orientation. To make the discovery of key-focuses more dependable, stable and efficient DoG Function G (x, y, σ) is required. Fig 2.9 demonstrates the DoG pyramid development of the approximate picture formed in the previous step.

The key-points that are at first distinguished on the approximate part of decomposed picture are appeared in the Figure 2.9 DoG image D is given by [19].

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) \times I(x, y)$$

$$= L(x, y, k\sigma) - L(x, y, \sigma) \quad \ldots 16$$

Where

$L(x, y, k\sigma)$ = convolution of the input picture

$G(x, y, k\sigma)$ = Gaussian blur

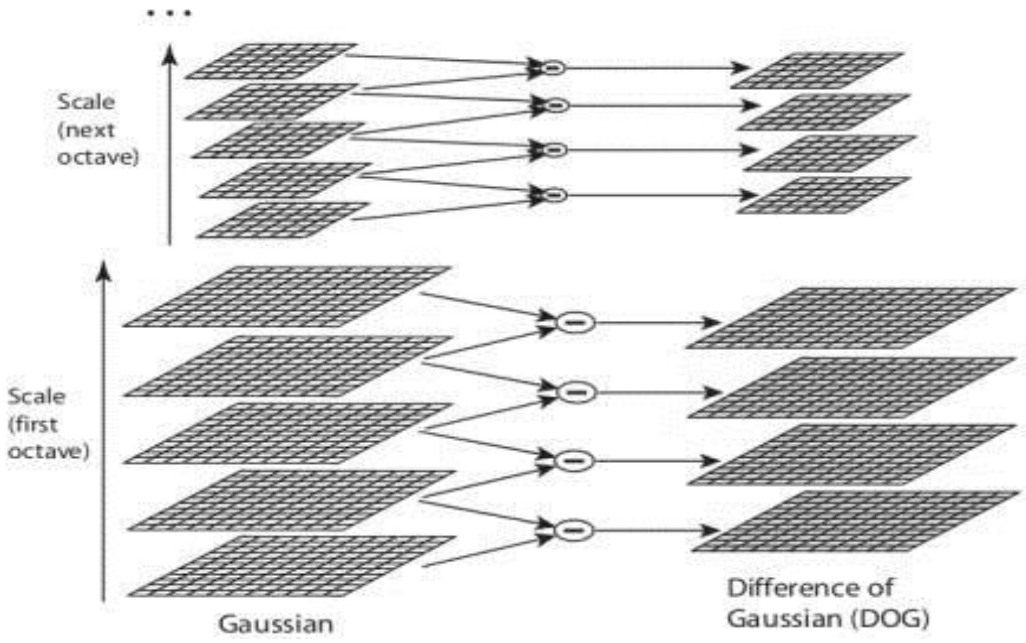


Fig 2.9 Pictorial representation of calculation of DOG of an image

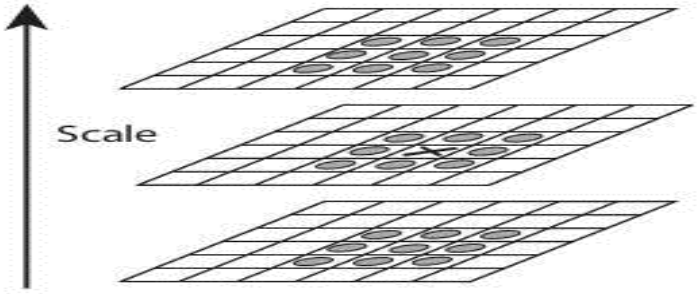


Fig 2.10 Pictorial representation to find out the maxima out of 26 neighbourhood pixel

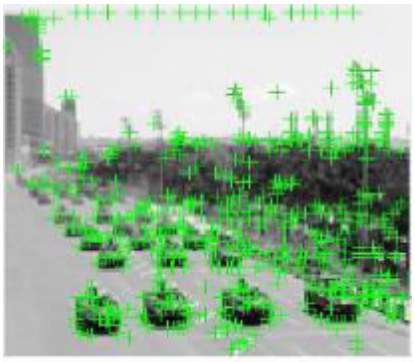


Fig 2.11 Initial position of the key points generated in the first step of SIFT i.e. with the help of DOG to find out scale space extrema of the given image

2. Localization of Key-point

In this process more exact key-points are chosen. For accomplishing this purpose, Taylor arrangement expansion of scale space is applied on it and those extrema which have intensity value lesser than the a pre-estimated edge value are rejected. The precisely chosen key-points on the approximate picture in the wake of disposing off the ones having poor difference are appeared in Figure 16. Taylor series expansion of scale space is used to obtain more correct location of extrema. The keypoint is rejected if the intensity of this extrema ies less than a predefined threshold value (normally 0.003). Edges also need to be removed as DoG has higher response for edges which uses Harris corner detector is used. For computation of principle curvature, it uses a 2x2 Hessian matrix (H). For every candidate key-point at coordinate , the Hessian matrix is calculated as follows:

$$H = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} \quad \ldots 17$$

Where,

h_{11} = p(i+1,j) + p(i-1,j) – 2p(i,j)

$h_{22} = h_{21}$ = p(i+1,j) + p(i,j-1) – 2p(i,j)

h_{22} = p(i+1,j+1) + p(i+1,j-1) – p(i-1,j+1) + p(i-1,j-1)/4

If $\frac{(h_{11}+h_{22})^2}{(h_{11}.h_{22})-h_{12}^2} < \frac{(c_{edge}+1)^2}{c_{edge}}$, then retain the key-point,otherwise discard it. Where c_{edge} is the ratio between the largest and non-zero smallest eigen-values in the block of the image. From Harris corner it is known that for edges, one value is larger than the other.

The keypoint is rejected if this ratio is higher than a threshold. Usually it uses 10 as a threshold. This step eliminates the low contrast keypoint and edge keypoint and the only accurate keypoint is obtained.

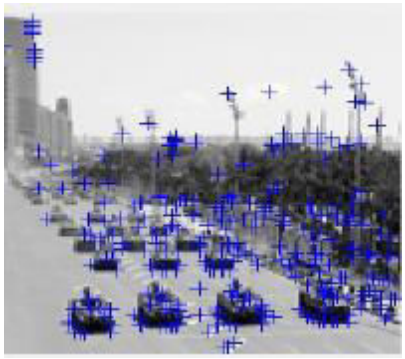


Fig 2.12 Precisely Selected Key-points generated in the second step of SIFT with the help of thresholding using Taylor series expansion

3. Assignment of Orientation

Each key-point is given an orientation as per the local image properties. To ascertain gradient direction of key-points, HOG is utilized. Predominant direction of the nearby gradient is shown by introduction of the histogram peaks.

The Magnitude of the gradient m(x, y) and orientation Θ(x, y) are calculated as: [15]

$$m(x, y) = ((L(x + 1, y) – L(x – 1, y))2 + (L(x, y + 1) – L(x, y − 1))2)1/2 \quad \ldots 18$$

$$\Theta(x, y) = \tan\text{-}1\ ((L(x, y + 1) – L(x, y − 1)) / (L(x + 1, y) – L(x – 1, y))) \quad \ldots 19$$

4. Key-point Descriptors Generation

The estimation of the local picture angle is taken at the chosen scale in the zone around each key-point. Key-point descriptors utilize an arrangement of 16 histograms each having 8 components. Hence the feature vector consists of total 128 number of feature vectors.

- Key-point Matching

The extricated key-points from SIFT methodology are utilized to discover a pool of coordinating sets of key-points. Euclidian distance is registered for finding the coordinated sets of key-points from a specific key-point to remaining all other key-points. This procedure is repeated iteratively and dependent on pre-estimated threshold value an arrangement of coordinated pairs are distinguished.

- Clustering

Agglomerative hierarchical clustering is utilized to aggregate the recognized coordinated pairs of key-points. A few Linkage strategies are utilized to finish the clustering procedure. On the off chance that something like two clusters having in excess of three coordinated pairs are discovered then the picture is considered as manipulated.

The linkage method operate as follows [9]:

$$\Delta dist(P, Q) = ESS(PQ) - [ESS(P) + ESS(Q)] \quad \ldots 20$$

Where,

$$ESS(P) = \sum_{i=1}^{np} |x_{Pi} - \_x_P|$$

- False Positive Matches Removal

In this progression we utilize an ordering tool named RANSAC to evacuate false positive matches. In this tool various discretionary pairs of points from the pool of matched pairs of points are chosen and contrasted and other remaining coordinated pairs as far as distance between them is considered. A threshold value is set and combines with distance inside the threshold value are considered as real coordinated pairs and others are rejected.

MIFT ALGORITHM

SIFT algorithm is unable to detect the cloned region of completely flipped clones, which is a common operation performed by criminals to hide the important details of the image of the witness to get away from the punishment of crime. Hence it has become really important in forensic analysis to work on this shortcoming of SIFT based technique to detect the 18o degree rotated cloned of the manipulated image.

MIFT technique is similar to SIFT based technique and is used to extract the key points of the picture. We know that a quality vector compose each key point and the neighborhood is used for the formation of the quality vector.

Descriptor is created using this vector. 4×4 matrix using 8 orientation bins are also modeled by it.128 dimension descriptor vector is selected same like SIFT in this technique.

- 16 cells order: As described in the previous section of this thesis, 16 cells are formed by SIFT.

  Both kind of flipping can be presented i.e. horizontal and vertical but in when we have the vertical flip, the order remains same. Thus there is no need to do anything except SIFT. We have focused in this thesis on the horizontal flipping of the image. Right and left directions are required to be selected. Direction is fixed based on the sum of all of the left and right position vectors.

$$m_r = \sum_{k=1}^{(N_{bin}-2)/2} L_{(n_d-k+N_{bin})\%N_{bin}}$$

$$m_l = \sum_{k=1}^{(N_{bin}-2)/2} L_{(n_d+k+N_{bin})\%N_{bin}} \qquad \ldots 21$$

Where,

N_{bin} = orientation bin number which is 36 in case of MIFT.

n_d= dominant orientation index

L_i = gradient magnitude

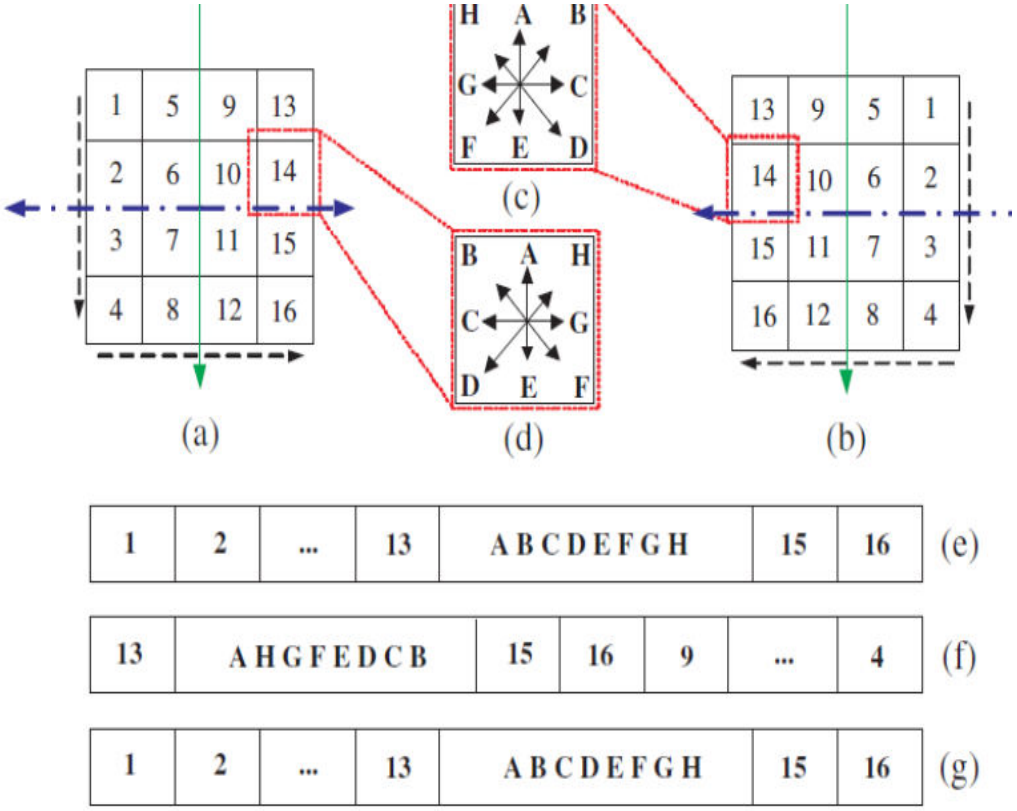


Fig 2.13 Feature vector of MIFT showing twice the number of features than SIFT

(a) = The keypoints in real picture

(b) = keypoints of flipped picture

(c) = 14th cell of b showing scattering

(d) = 14th cell of a showing scattering

(e) = a's descriptor

(f) = b's SIFT descriptor

(g) = b's MIFT descriptor

- 8 Orientation order : reorganizing the order of the bins is the other way. Values of m_l and m_r are required for this. The above figure shows it when it is rotated in anticlockwise and clockwise direction respectively.

After calculation of MIFT of the approximate image computed using SWT, we need to proceed same as in the previous technique of SIFT.

Thus we have now better descriptor than SIFT which contains better information which is used to compute the localization of the cloning of the completely 180 degree flipped images.

After calculation of MIFT key points following steps are used to detect the forged image:

1 Clustering and Matching of the extracted key points

2 False positive clusters removal using RANSAC

3 Localization of forged regions of the image

CHAPTER 3 RESULTS

DCT ALGORITHM

This DCT algorithm was tested with many input test images. The algorithm is working well on pictures with cloned regions that do not generate rotation or scale.

Figure 17 shows the DCT algorithm is running on a crime scene picture with five objects shown on pavement. Despite the correlation of the pavement, when using a threshold of 10 and a quality factor of 0.5, the algorithm was correctly able to identify that the fifth object had been covered. In the output image, the copied region is highlighted and shown as the purple region being copied and moved to the green region (or vice-versa).

Fig 3.1 Left: Original picture; Middle: Input picture; Right: Output picture with threshold 10 and quality factor 0.5

Another example is given in Figure 3.1. In this figure, the middle image shows the result of the American flag on the right side of the picture being copied and pasted above the telephone pole.

With quality factor 0.35 and threshold 27, the algorithm was able to correctly identify the flag in purple as the copied moved region. In some tests, the algorithm would be able to recognize the forged region but also incorrectly identify regions that were flat like a grassy field or the sky. These regions would get highlighted by the algorithm almost randomly and appear as noise in the output.

Fig 3.2 Left: Original picture; Middle: Input picture; Right: Output picture with threshold 27 and quality factor 0.35

An example where this happened is given in Figure 3.2. In Figure 3.3, the person was copied with a rectangular region to the left and the shadow of the person was copied with a rectangular region below the shadow. Using a threshold of 32 and a quality factor of 0.745, the algorithm was able to identify in blue and green the two copy-moved regions. However, due to the false positives that appear as noise in the output, this example shows the need for human interpretation of the data from a CMFD algorithm.

In tests that included even a slight rotation in the copied region, the algorithm does not detect any of those regions as a possible forged region. This result is demonstrated in Figure 3.6. Figure 3.6 shows the same crime scene photo as before except instead of a region being copied and directly moved overtop of the number 5, the copied region was

rotated first by 180 degrees and then placed over the number 5. The results were the same for any variation of rotation greater than 0 degrees and zero shift vectors were identified. The algorithm also was unable to identify images where the copied region was scaled in any way. Hence due to these shortcomings we moved towards the feature based methods which are comparatively better on detecting the cloned regions of the image after geometric rotation or scaling technique has been applied on the given segment of the image before pasting it on the input image to change some of the characteristics of this image.

Fig 3.3 Left: Original image; Middle: Input image

Figure 3.5 demonstrates the algorithms inability to identify scaled regions. In this figure, the same crime scene photo is used.

The region boxed in red in the image on the left was copied, scaled to 175% its original size, and then moved over numbers 3, 4 and 5. With this input, zero shift vectors were identified. Similarly, for scaling of 125%, 150%, and 200% the algorithm identified zero shift vectors.

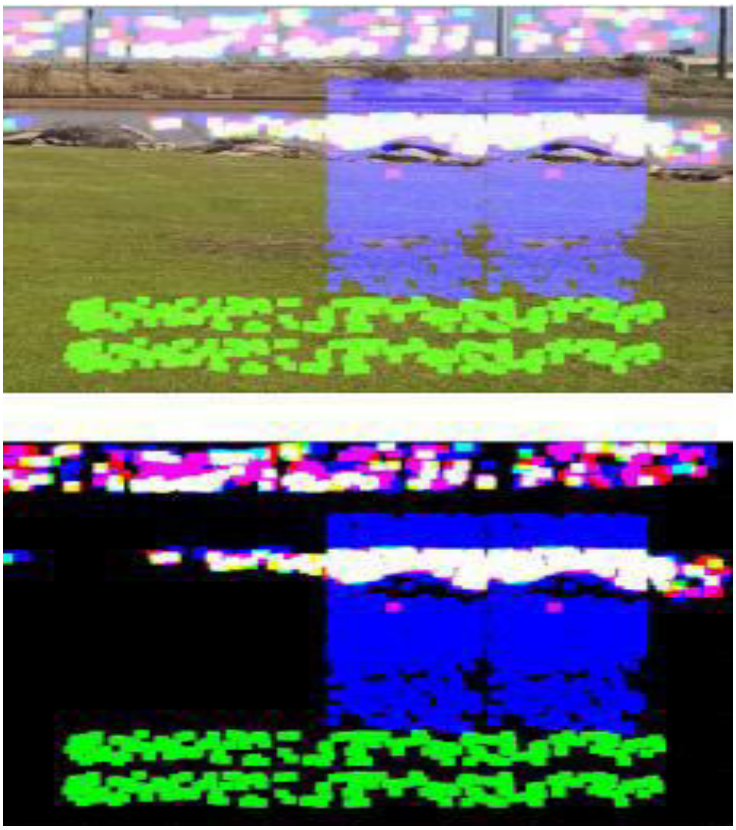


Fig 3.4 Top Right: Output image with threshold 32 and quality factor 0.745; Bottom Right: Test image showing only the regions that were highlighted

Fig 3.5 Left: Original image with box around the region that will be copied; Middle: Input image where the highlighted region from left was scaled by 150% and used to cover numbers 3, 4, and 5. Right: Output image showing no highlighting, quality factor 0.75 and threshold 10.

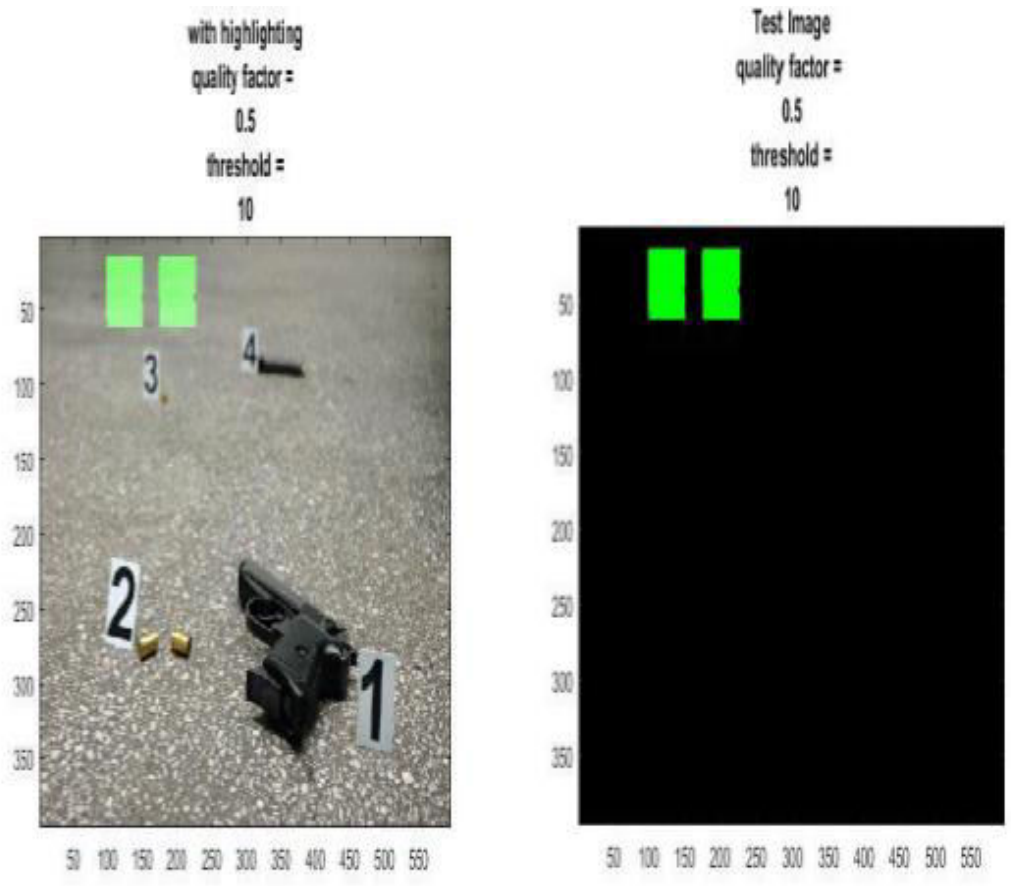


Fig 3.6 Inability to detect the degree of rotation when the segment is flipped by 180 degree and placed on the given picture.

SIFT ALGORITHM

We applied this algorithm over the standard dataset MICC-F220.

Firstly, 2-D SWT is applied on the images of the dataset and approximate component of the decomposed picture is provided as the input image in SIFT algorithm to extract the descriptor vectors for this image.

Finally, coordinating operation is performed on the extracted key-points in order to find out the localized regions of the cloning.

Fig 3.7 Shows an input image which is forged as the bird is copied and moved to another place.

When the SIFT dependent cloning forgery detection method is used on this input image various DOG pyramids are formed which are shown in Fig 3.8 and Fig 3.10. These are the basis for the generation of the features on the input image. The features are further used for the detection of cloned parts of the image.

Fig 3.8 DOG of given input

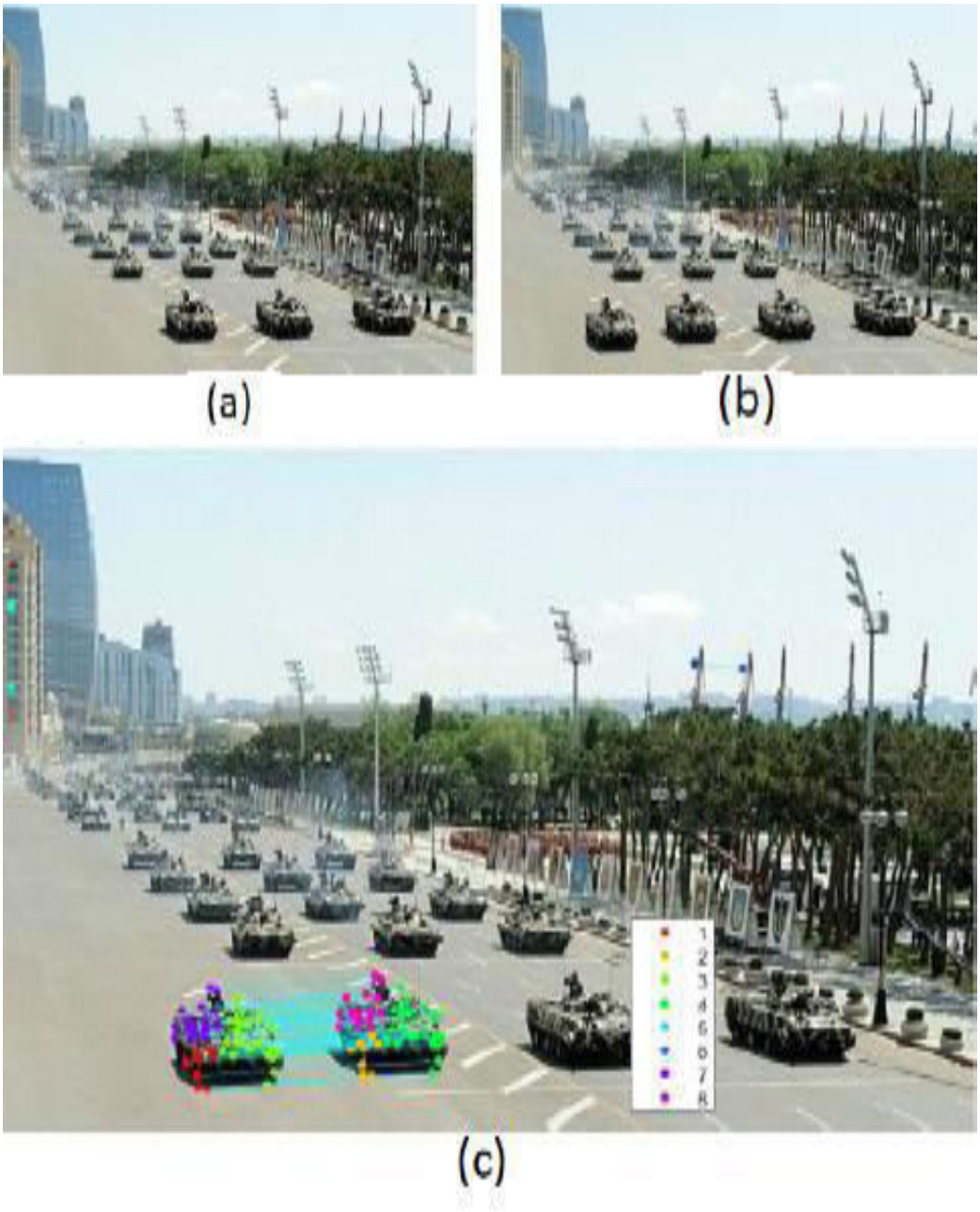


Fig 3.9 (a) Real, (b) Cloned, (c) Cloning Detection

Fig 3.9 shows the output of another image which is forged and a segment is copied and moved to another part and is detected effectively by the SIFT based technique.

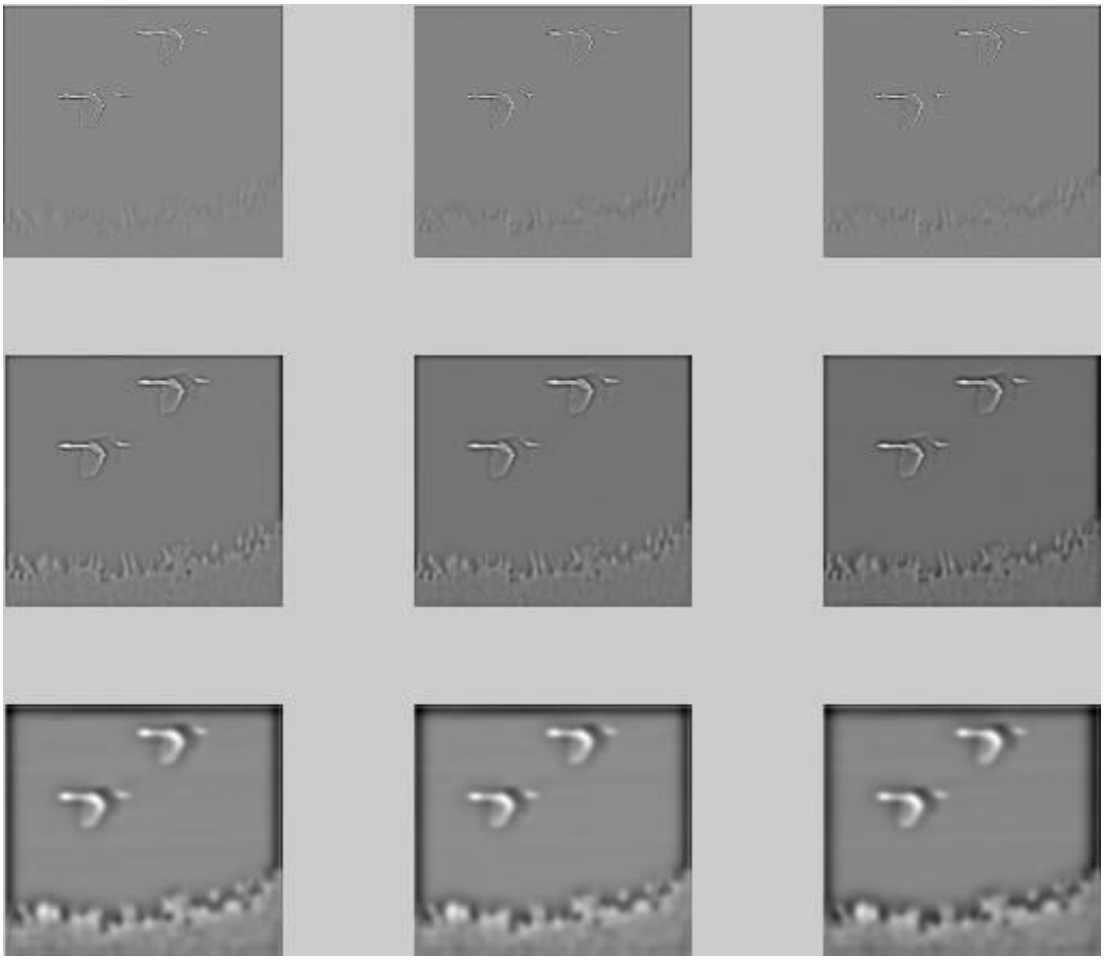


Fig 3.10 DoG Pyramids of Approximate Components

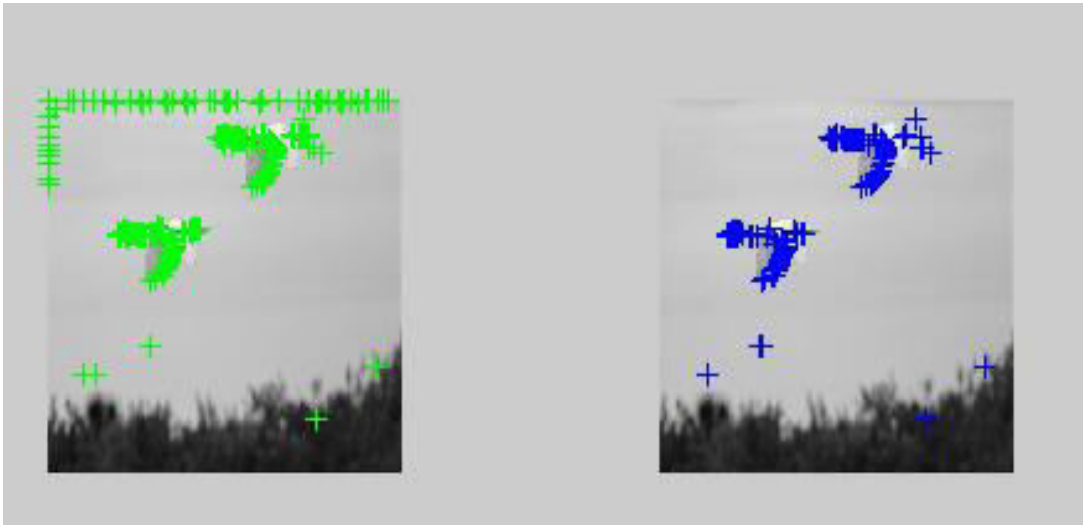


Fig 3.11 Final output of SIFT based technique

MIFT ALGORITHM

We applied this algorithm over the previous dataset after flipping the copied portion by 180 degree.

Firstly, 2-D SWT is applied on the images of the dataset and approximate component of the decomposed picture is provided as the input image in MIFT algorithm to extract the descriptor vectors for this image.

Finally, coordinating operation is performed on the extracted key-points in order to find out the localized regions of the cloning.

Fig 3.12 Shows an input image which is forged as the bird is copied and moved to another place while flipping it with 180 degree

When the MIFT dependent cloning forgery detection method is used on this input image various DOG pyramids are formed. These are the basis for the generation of the features on the input image. The features are further used for the detection of cloned parts of the image.

Fig 3.13 DOG of given input

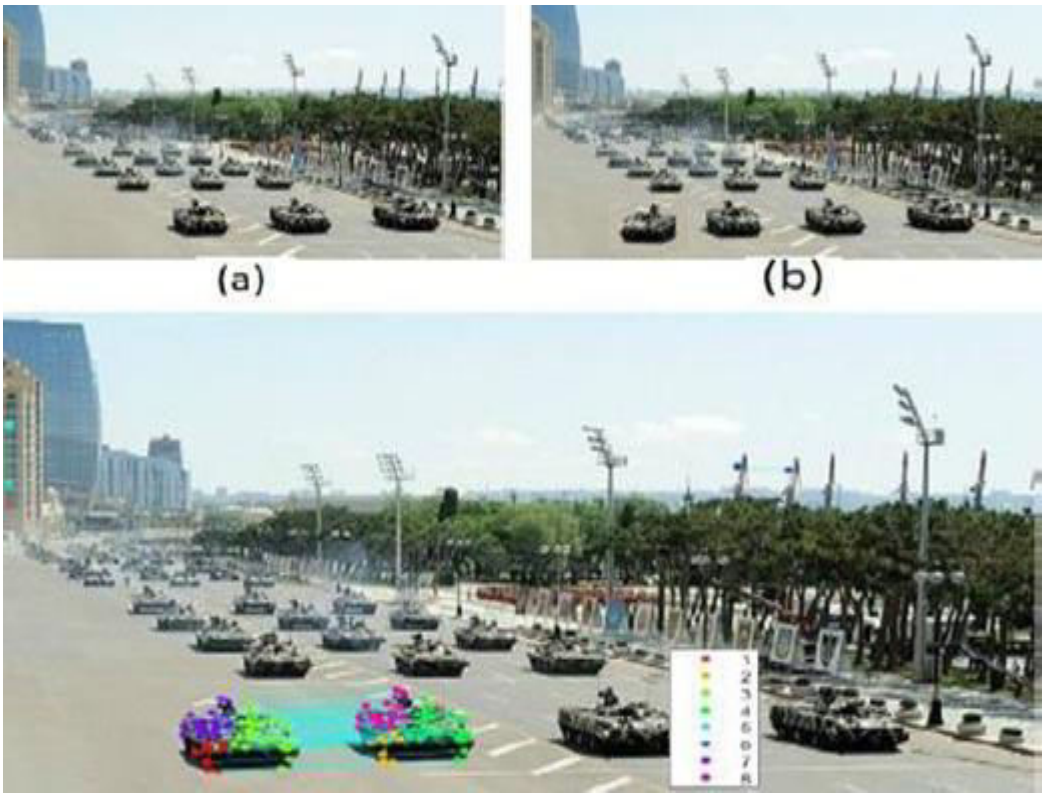


Fig 3.14 (a) Real, (b) Cloned, (c) Cloning Detection

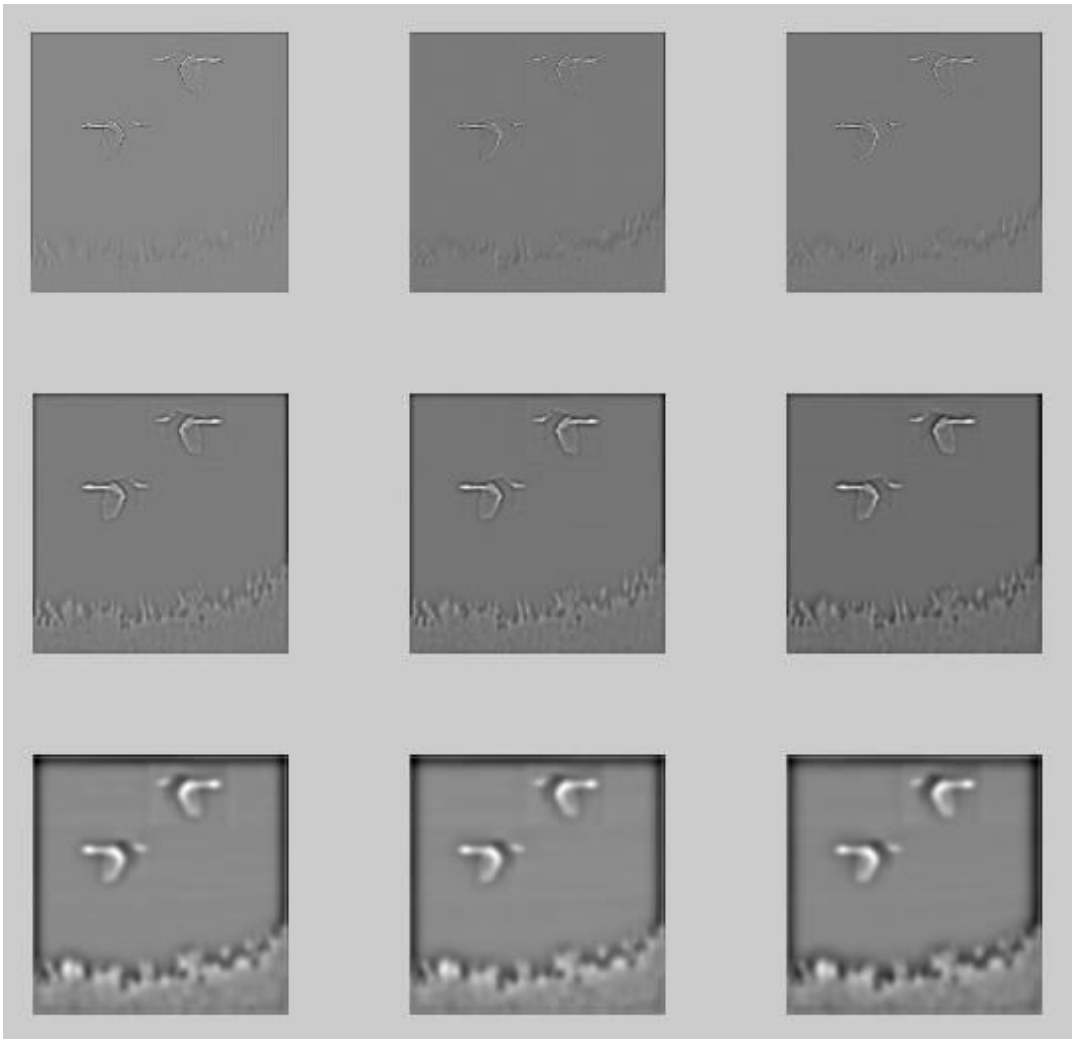


Fig 3.15 DoG Pyramids of Approximate Components

Fig 3.16 Final output of MIFT based technique

Fig 3.17 Shows an input image which is forged with resizing

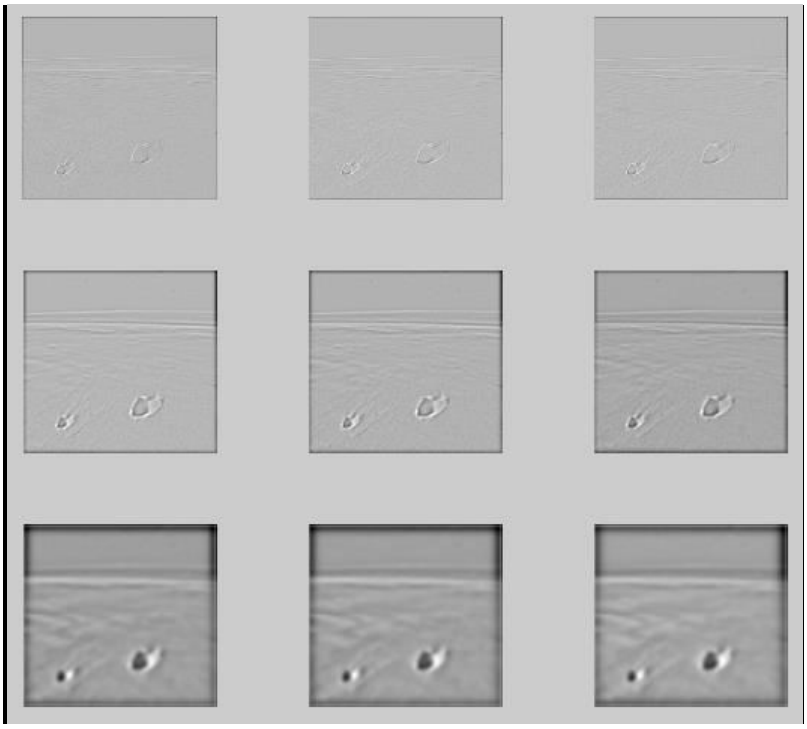


Fig 3.18 DoG Pyramids of Approximate Components

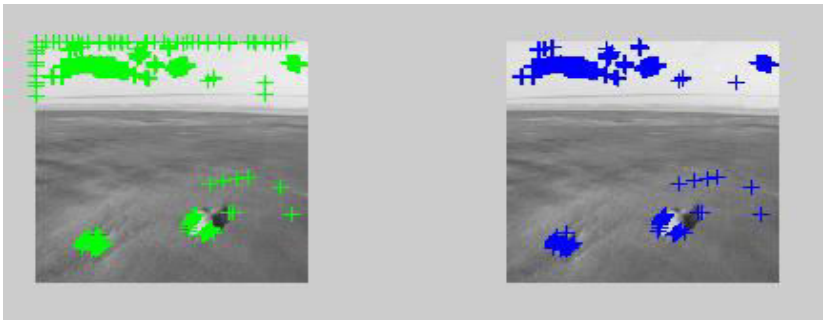


Fig 3.19 Final output of MIFT based technique

Fig 3.20 Shows an input image which is forged with rotation

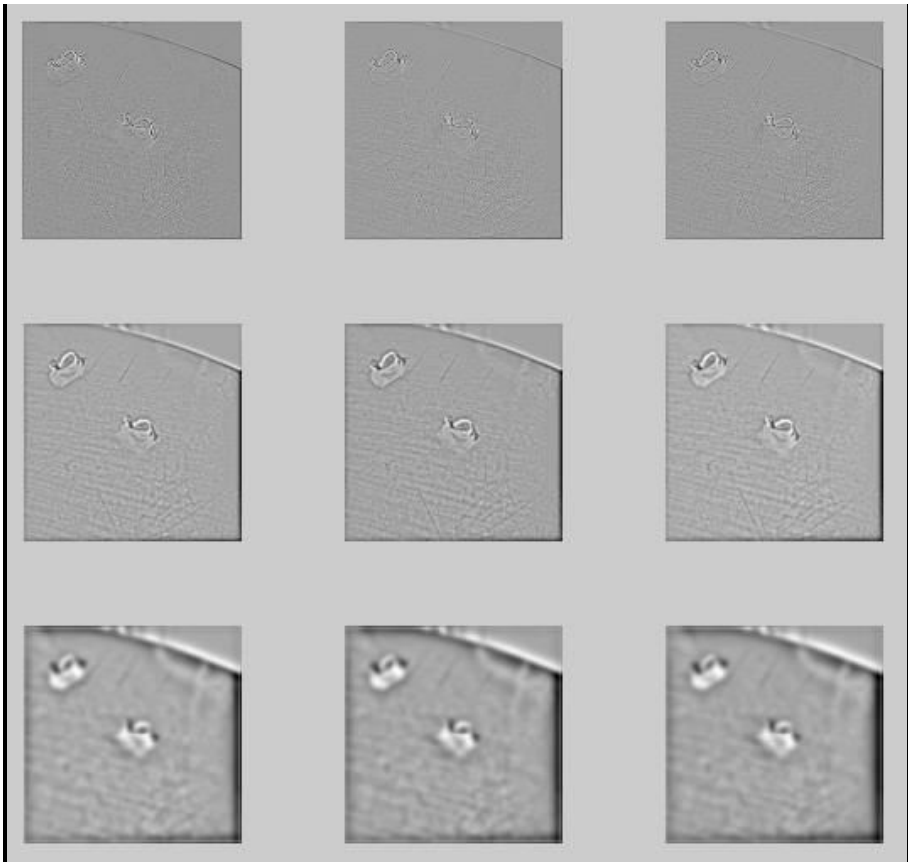


Fig 3.21 DoG Pyramids of Approximate Components

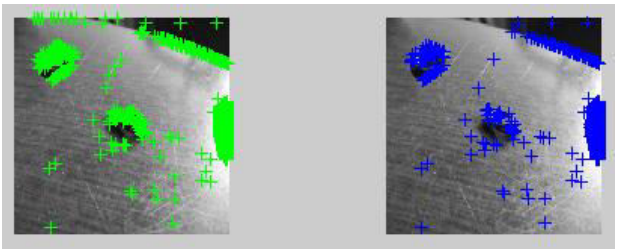


Fig 3.22 Final output of MIFT based technique

Fig 3.23 Shows an input image which is forged with resizing

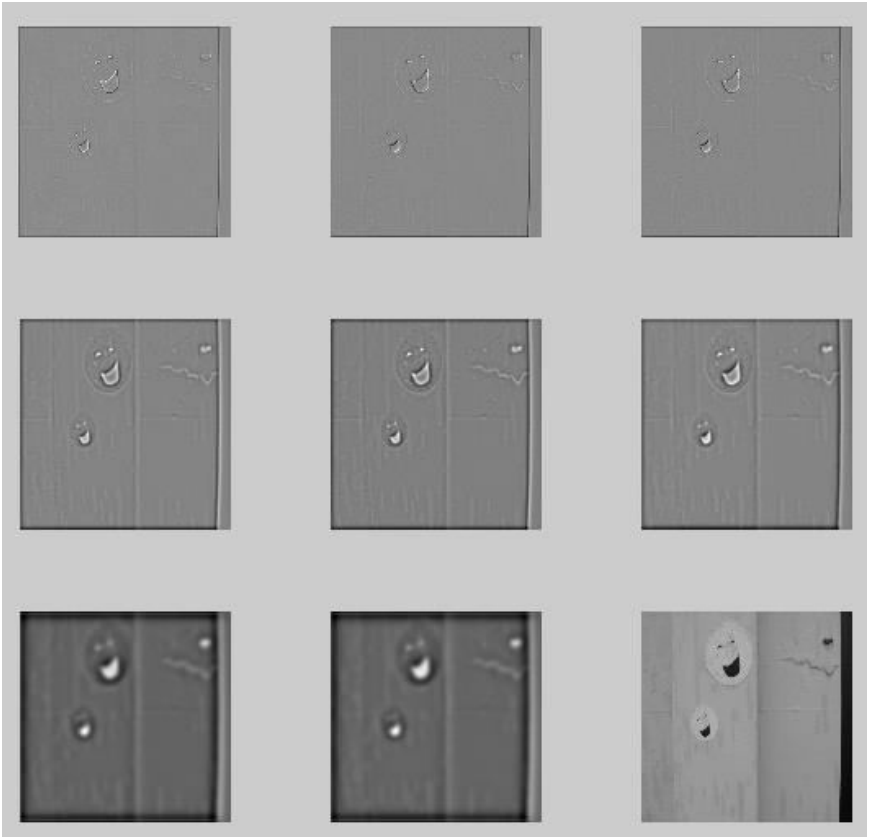


Fig 3.24 DoG Pyramids of Approximate Components

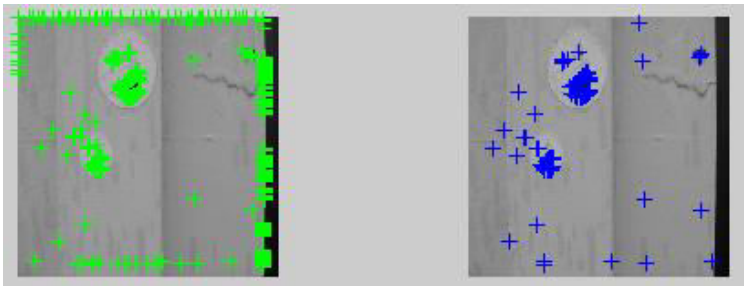


Fig 3.25 Final output of MIFT based technique

COMPARISON BETWEEN FEATURE BASED TECHNIQUES AND DCT :

- ❖ We found out that the feature based technique to determine the cloned images is better than the DCT based technique as feature based technique is able to detect the copied parts that are scaled or rotated and then pasted to any other part of the image.

- ❖ The detection of false positives is further less in comparison to DCT based technique.

- ❖ Feature based technique is better when one part of image is repeated, whereas DCT based technique will provide better result when one important segment of the image is hidden using other part of the same image.

- ❖ Feature based technique is more reliable then DCT technique.

EXPERIMENTAL PARAMETERS USED IN THE COMPUTATION

The parameters we had utilized for portraying the examination are as underneath:

- True Positive (TP): True positive demonstrates number of pictures effectively recognized as cloned.
- True Negative (TN): Indicates number of pictures effectively distinguished as non-altered.
- False Positive (FP): Indicates number of pictures unsuccessfully recognized as altered while really the pictures are not altered.
- False Negative (FN): Indicates number of picture unsuccessfully recognized as non-altered.
- Accuracy: Accuracy gives the ratio of really distinguished pictures from total number of pictures.

Accuracy = $\frac{TP+TN}{TP+FP+TN+FN}$

- True Positive Rate (TPR): It computes the percentage of pictures successfully detected as altered. It is measured as:

TPR = $\frac{TP}{TP+FN}$

- False Positive Rate (FPR): Indicates the percentage of non-altered pictures which are unsuccessfully identified as altered one. It is measured as:

FPR = $\frac{FP}{FP+TN}$

Table 3.1 Performance analysis Factors

Abbreviation	Full Form	Meaning
TP	True Positive	Cloned Image Detected as Cloned
FP	False Positive	Authentic Image Detected as Cloned
TN	True Negative	Authentic Image Detected as Authentic
FN	False Negative	Cloned Image Detected as Authentic

Table 3.2 Outcome of proposed method

No. of original images	No. of cloned images	TP	TN	FP	FN
50	50	47	47	1	5

Table 3.3 Performance of proposed method

Specificity	Accuracy	FPR%	FNR%	TPR%
97.91%	94%	1%	20%	90.38%

Table 3.4 Comparison of performance based on different attacks on image

Types of attack	Number of key points found	Computational time(s)
No rotation and scaling	397	12.81
Scaling	376	18.57
Rotation	259	7.52
Scaling and rotation	287	14.44

FUTURE WORK

The above methodologies have different advantages as they can manage a wide range of geometric changes, deformation and blurring. The space and time required for calculation is additionally less contrasted with block based techniques. Yet at the same time there are issues as referenced beneath.

- These approaches don't work for flat portions of the image.
- High false positive rate of the recognition results is likewise a noteworthy issue and should be managed.
- Proper method for clone localization isn't available.
- Computational efficiency is less and thus there is the scope for improvement
- It cant be used for the detection of very small clones.

The different methodologies mentioned in the thesis for keypoint based cloning recognition cant be applied on digital videos.The FPR and time taken is high, which makes the accuracy to be very low.

Further detecting video forgery is relatively less explored area and as we saw recently there were numerous incidents of mob lynching due to forged videos and images spamming on whatsapp.

Fig 3.26 Original image and its modified picture with splicing effect.

So there is an urgent need to classify the image as forged or real on these social networking platforms to tackle this growing worldwide problem.

If technology is the reason for the death of innocent people, the technology can only solve this problem and further with the growth of various government initiatives like Digital India, a common man has the access of a digital device which leads to further high requirement of regularizing image and video forgery in this digital era and we have already discussed about its extensive use in the forensic science.

The study can be further extended to increase its domain towards detection of cloning in Digital videos and cloned images using splicing technique.There is a urgent need to research in this area as it will have significant effect on forensic science and is able to completely transform the current way to detect image and video cloning in forensic science.

APPENDICES

- Cloning
- Image retouching
- Splicing
- Watermarking
- Non Blind approach(active)
- Blind approach(passive)
- Edge map generation
- Color component separation
- Histogram generation
- Frequency transform of Histogram
-Pixel

2.1- Exhaustive search equation

2.2- Equation for Autocorrelation

2.3- Marr edge detector

2.4- Exact Match

2.5-Robust Match

2.6-Shift Vector

2.7- Q-Factor

2.8- SWT-SVD

2.9-SIFT Algorithm

2.10- RANSAC

2.11- Unit Matrix

2.12- RGB to Greyscale conversion

2.13-swa

2.14-Taylor series expansion

2.15- DOG

2.16-Autocorrelation using Fourier Transform

2.17-Keypoint localization

3.1 True Positive

3.2 False Positive

3.3 True Negative

3.4 False Negative

3.5 Accuracy

3.6 TPR

3.7 FPR

3.8 Sensitivity

3.9 Specivity

REFERENCES

[1] Anil Dada Warbhe, Rajiv V. Dharaskar, Vilas M. Thakare, “Block Based Image Forgery Detection Techniques”, International journal of engineering sciences and research technology, 289-297, August 2015.

[2] W. Luo, J. Huang, and G. Qiu, Robust detection of region duplication forgery in digital images, in Proc. Int. Conf. on Pattern Recognition, Washington, D.C., pp. 746749, 2006.

[3] S. Kumar and P. K. Das, Copy-Move Forgery Detection in digital Images: Progress and Challenges, International Journal on Computer Science and Engineering, Vol. 3, No. 2, pp. 652-663, February 2011.

[4] R. Granty, T. Aditya, and S. Madhu, Survey on passive methods of image tampering detection, in Communication and Computational Intelligence (INCOCCI), 2010 International Conference on, pp. 431 436, Dec. 2010.

[5] CASIA Image Tampering Detection Evaluation Database, Ver. 2.0, 2010,http://forensics.idealtest.org.

[6] J. Zhang, Z. Feng, Y. Su, A new approach for detecting copymove forgery in digital images, IEEE Singapore International Conference on Communication Systems, pp. 362366, 2008

[7] B. Mahdian and S. Siac, A bibliography on blind methods for identifying image forgery, Signal processing: Image Communication, pp. 389-399, 2010.

[8] Shaid, S.Z.M.: “Estimating optimal block size of copy-move attack detection on highly textured image”. Thesis Submitted to the University of Technology, Malaysia, 2009.

[9] Farid, H.: “Digital doctoring: how to tell the real from the fake”, Significance, 3, (4), pp. 162166, 2006

[10] Krawtez, N.: “A pictures worth digital image analysis and forensics”. Black Hat Briefings, pp.131, 2007. Available at www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf.

[11] V. Christlein , C. Riess and E. Angelopoulou , ”On rotation invariance in copy-move forgerydetection” , Proc. IEEE Workshop on InformationForensics and Security , pp.129 -134 , 2010

[12] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, A SIFTbased Forensic Method for Copy-Move Attack Detection and Transformation Recovery, IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 10991110, Sep. 2011.

[13] H. Huang, W. Guo, And Y. Zhang, ”Detection Of Copy-Move Forgery In Digital Images Using Sift Algorithm,” In Computational Intelligence And Industrial Application, 2008. Paciia’08. Pacific-Asia Workshop On, Pp. 272-276, 2008.

[14] X. Bo, W. Junwen, L. Guangjie, And D. Yuewei, ”Image Copy- Move Forgery Detection Based On Surf,” In Multimedia Information Networking And Security (Mines), 2010 International Conference On, Pp. 889-892, 2010.

[15] Zheng, J., Haoa, W., and Zhub, W. Detection of Copy-move Forgery Based on Keypoints Positional Relationship*. Journal of Information and Computational Science, 1(3), 53-60, 2012.

[16] Jaberi, Maryam, George Bebis, Muhammad Hussain, and Ghulam Muhammad. ”Accurate and robust localization of duplicated region in copymove image forgery.” Machine vision and applications 25, no. 2: 451- 475, 2014.

[17] X. Guo and X. Cao. Mift: A mirror refection invariant feature descriptor. In ACCV, volume 2, pages 536-545, 2009.

[18] M. A. Fischler and R.C. Bolles. Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography, Communications of the ACM 1981.

[19] D. G. Lowe. Distinctive image features from scale-invariant keypoints. IJCV, 60(2):91-110, 2004.

[20] J. Li, X. Li, B. Yang and X. Sun, “Segmentation-Based Image Copy-Move Forgery Detection Scheme,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015.

[21] T. Mahmood et al., "A survey on block based copy move image forgery detection techniques," *2015 International Conference on Emerging Technologies (ICET)*, Peshawar, pp. 1-6, 2015.

[22] T. K. Huynh, K. V. Huynh, T. Le-Tien and S. C. Nguyen, “A survey on Image Forgery Detection techniques,” *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies - Research, Innovation, and Vision for Future (RIVF)*, Can Tho, pp. 71-76, 2015.

[23] V. T. Manu and B. M. Mehtre. “Detection of copy-move forgery in images using segmentation and SURF,” *Advances in Signal Processing and Intelligent Recognition Systems*, vol. 425, pp. 645-654, 2016.

[24] N. P. Joglekar and P. N. Chatur, “A Compressive Survey on Active and Passive Methods for Image Forgery Detection,” *International Journal of Engineering & Computer Science*, vol. 4, no. 1, pp.10187-10190, 2015.

[25] S. Prasad and B. Ramkumar, “Passive copy-move forgery detection using SIFT, HOG and SURF features,” *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, pp. 706-710, 2016.

[26] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy-move forgery indigital images,” in *Proceedings of the Digital Forensic Research Workshop*, 2003.

[27] A. C. Popescu and H. Farid, “Exposing Digital Forgeries By Detecting Duplicated Image Regions,” Rep. TR2004-515, Dartmouth College, Computer Science, Hanover, Conn, USA, 2004.

[28] M. F. Hashmi, V. Anand and A. G. Keskar, “Copy-Move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform,” *Aasri Procedia*, vol. 9, pp. 84-91, 2014.

[29] R. Dixit, R. Naskar and S. Mishra, “Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD,” *IET Image Processing*, vol. 11, no. 5, pp. 301-309, 2017.

[30] D. G. Lowe, “Distinctive Image Features from Scale-Invariant Keypoints,” *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004.

[31] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, “A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.