Digital Tampering Detection Techniques: A Review

Kusam[1], Pawanesh Abrol[2] and **Devanand[3]**

Abstract - ***In this era of digital computing, the interest and necessity of representing information in visual forms has become very important. Due to considerable improvement in computing and network technologies, and the availability of better bandwidths, the past few years have seen a considerable rise in the accessibility, sophistication, and transmission of digital images using imaging technologies like digital cameras, scanners, photo-editing, and software-packages. However, this technology is also being used for manipulating digital images and creating forgeries that are difficult to distinguish from authentic photographs. Tampering of images involves pasting one part of an image onto another one, skillfully manipulated to avoid any suspicion. Any image manipulation can become a forgery, based upon the context in which it is used. The sophisticated and low-cost tools of the digital age enable the creation and manipulation of digital images without leaving any perceptible traces. As a result, the authenticity of images can't be taken for granted, especially when it comes to legal photographic evidence. Manipulations on an image encompass processing operations such as scaling, rotation, brightness adjustment, blurring, contrast enhancement, etc. or any cascade combinations of them. Thus the problem of establishing image authenticity has become more complex with easy availability of digital images and free downloadable image editing softwares leading to diminishing trust in digital photographs. Detecting forgery in the digital images is one of the challenges of this exciting digital age. A lot of research is underway to detect and prevent forgery in digital images. One of the problems in web based image applications is non-availability of original image for evaluation. Further, digital imagery authentication techniques based on cryptographic principles and digital signatures offer no modification protection following image transmission. In this paper, we study the major approaches to detect forgery in digital images. Initially, the process of digital image tampering is explained. Subsequently, we analyze some of recent algorithms for detecting digital forgery including copy-move, chromatic aberration, PCA for detecting duplicated image, lighting inconsistencies. Preliminary investigations show that different algorithms have different domains of tampering detection and have different merits and demerits. The decision about the content authenticity is complex and can b better established by interpreting the results obtained by applying a set of these methods.***

Index Terms - Digital Image, Digital Forgery, Digital Tampering.

1. INTRODUCTION

An image is a two-dimensional function, f(x,y), where x and y are spatial (plane) coordinates and the value of f(x,y) at any pair of coordinates (x,y) is called the intensity or gray level of the image at that point. An image contains a lot of information and can be monochromatic or colored. When the digital technology is used to capture, store, modify, or view images, they must be first converted into numbers: 1s and 0s called bits. A combination of eight bits is called a byte. A digital image is composed of a finite number of elements which are referred to as pixels. A pixel is a basic unit of a colored or monochromatic image on a computer display or in a computer generated image. A common color image file of size 1024 X 1024 pixels and 256 colors (or 8 bits per pixel) occupies 3MB of disk or RAM space. Since a colored image contains more information (coloring details), so its file size is comparatively much larger than that of monochrome. Digital images are typically stored in either 24-bit or 8-bit files. Color variations for the pixels are derived from three primary colors: red, green, and blue. Each primary color is represented by 1 byte; 24-bit images use 3 bytes per pixel to represent a color value. These 3 bytes can be represented as hexadecimal, decimal, and binary values [3].

In contrast to analog signal processing in which the image signal is treated as a continuous signal, digital image processing has many advantages. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Digital image formation, the foremost step in any digital image processing application, consists basically of an optical system, a sensor and a digitizer. The optical signal is usually transformed to an electrical signal by using a sensing device (e.g. a Charge Coupled Device sensor). The analog signal is transformed to a digital one by using a video digitizer (frame grabber). Thus, the optical image is transformed to a digital one. Due to inherent limitations of the processing systems, each digital image formation subsystem may introduce a deformation or degradation to the digital image (e.g. geometrical distortion, noise, non-linear transformation etc.). The mathematical modeling of the digital image formation system is very important in order to have precise knowledge of the degradations introduced. After conversion of the image to binary data stream, it is put back together in a grid of small squares. These tiny squares also called sample space are the pixels, and are the building blocks of all the computer graphics and images. The values in the pixels indicate the intensity level associated with that pixel.

[1]*Research Scholar, Deptt. of Computer Science & IT, University of Jammu*
[2]*Sr. Asstt. Professor, Deptt. of Computer Science & IT, University of Jammu*
[3]*Professor & Head, Deptt. of Computer Science & IT, University of Jammu*
E-Mail: [1]*kusam2univ@yahoo.co.in and*
[2]*pawanesh_a@yahoo.com*

There has been wide availability of the different powerful image processing and editing software with help of which the digital images can be easily manipulated. Many of these software are freely available and often do not require any special skills to operate. A digital image can be enlarged, enhanced, backgrounds, color contrasts and color schemes can be altered, even facial features can be changed to some other person's appearance. Images can be converted from one image format to another and any part of image can be altered pixel by pixel. Before the digital age, it was fairly easy to detect the altered photographs. But now with the advent in the commercial softwares, the tampering of the photographs have become very easy, can be carried out without any obvious signs of tampering and it is becoming harder to uncover and spot the authentic ones. With the increased reliance on digital images for information, the need to ensure their authenticity increases as well. Research in the field of image authenticity is still in its infancy state. +Recently, research on digital image forensics has gained attention by addressing forgery detection and image source identification. Both static images as well as video can be manipulated. However, in the current paper, we have discussed the digital forgeries related to static digital images only.

Any image manipulation can become a forgery, based upon the context in which it is used. An image altered for fun or someone who has taken a bad photo, but has been altered to improve its appearance cannot be considered a forgery even though it has been altered from its original capture. On the other side, some people creates a forgery for gain and prestige and to make the recipient believe that the image is real and not the fake one. Three types of forgeries can be identified:

a) Using Graphical Software is one method in which a forged image can be created. It especially needs a skilful creator who can ensure that the image he is creating is realistic, e.g. that the fall of light on objects in an image is consistent right across the image, that shading is consistent, the absorption of light by an object etc. An image created using this method takes some time to develop.
b) Creating an image by altering its Content is another method. In this, the recipient is duped to believe that the objects in an image are something else from what they really are. The image itself is not altered, and if examined will be proven as so.

Creating an image by altering its Context is the third method. In this, objects are removed or added from an image resulting in copy-move forgeries. E.g. a person can be added or removed. The easiest way is to cut an object from one image and insert it into another image. Various image / photo editing softwares like Adobe Photoshop, XnView, ProShow Gold etc. make this a simple task [6].

An example of a digital forgery is shown in Figure 1. As the newspaper cutout shows, three different photographs were used in creating the composite image: Image of the White House, Bill Clinton, and Saddam Hussein. The White House was rescaled and blurred to create an illusion of an out-of-focus background. Then, Bill Clinton and Saddam were cut off from two different images and pasted on the White House image. Care was taken to bring in the speaker stands with microphones while preserving the correct shadows and lighting. Figure 1 is, in fact, an example of a very realistic looking forgery [7].


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

BY DANIEL VERTON

ALTERED IMAGE

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.

Figure 1:Example of a Digital Image Forgery

With this increased reliance on digital images for information, the need to ensure their authenticity increases as well. The manipulation of images through forgery influences the perception an observer has of the depicted scene, potentially resulting in ill consequences if created with malicious intentions. This poses a need to verify the authenticity of images originating from unknown sources in absence of any prior digital watermarking or authentication technique. Authentication of digital images plays an important role in forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services and journalism.

There have been quite a few techniques proposed in combating the tampering of digital images. The digital camera computes a cryptographic hash of the image, and encrypts the hash using the private component of the key, which is built into the camera. The encrypted hash is then stored along with the digital image. Another complementary approach is to use digital time-stamping / digital signatures. These schemes effectively protect the data from modification during transmission, but they offer no protection following transmission. Since the information needed for these schemes to perform the authentication is separate from the data. An attacker can simply modify the data, recalculate the new message digest or digital signature, and attach them together.

Without knowledge of the original data or of the original authentication information, it is impossible to contest the authenticity of the modified digital image. Since the value of digital images is based on its content, the image bits can be modified to embed codes without changing the meaning of its content. Once the codes are embedded in the data content and the data is manipulated, these codes will also be modified so the authenticator can examine them to verify the integrity of the data. [8]

The widely used approach to verify an image's authenticity is to embed checksums into the least significant bits (LSB) of the image. A secret numeric key known by both the sender and the recipient protects these checksums. Another cost effective way to authenticate picture is through the use of metadata, although the information gathered from Metadata cannot stand on its own, as metadata is not strictly bound to a file, but it can provide useful information if it is used in the proper context.

The process of detecting image tampering is supposed to be carried out in six stages. The first five stages correspond to major theoretical goals of the process, the last one is related to real-life applications, a) blind method for resampling detection, b) blind method for duplicated regions detection, c) detection of discrepancies in lighting conditions and brightness levels, d) automatic method for detection of double JPEG compression, e) detection of inconsistent noise patterns, f) system integration and testing. Overall, these methods proved encouraging in detecting image forgeries with an observed accuracy of 60%.

Also, Digital watermarks have been proposed as a means for fragile authentication, content authentication, detection of tampering, localization of changes and recovery of original content. While digital watermarks can provide useful image before the tampering occurs. This limits their application to controlled environments that include military systems or surveillance cameras. Unless all digital acquisition devices are equipped with a watermarking chip, it will be unlikely that a forgery-in the-wild will be detectable using a watermark. It might be possible, but very difficult, to use unintentional camera "fingerprints" related to sensor noise, its colour gamut, and / or its dynamic range to discover tampered areas in images. Another possibility for blind forgery detection is to classify textures that occur in natural images using statistical measures and find discrepancies in those statistics between different portions of the image. At this point, however, it appears that such approaches will produce a large number of missed detection as well as false positives.

In this research work we have studied the techniques and methods of Digital Image Forgery Prevention and Detection Mechanisms. Also, we have reviewed the forgery detection method using Block Matching techniques of Copy-move algorithm [7, 11]. In the next section, we discuss some of the algorithms which have been presented by different researchers for detection of digital image tampering. Under Results & Discussion, we investigate and comparatively analyze some of the algorithms on the basis of the merits, demerits, input, output and space & time complexity. We present the conclusion and the future directions in which we are working.

2. LITERATURE REVIEW

The sophisticated and low-cost tools of the digital age enable the creation and manipulation of digital images without leaving any perceptible traces. As a result, the authenticity of images can't be taken for granted, especially when it comes to legal photographic evidence. Manipulations on an image encompass processing operations such as scaling, rotation, brightness adjustment, blurring, contrast enhancement, etc. or any cascade combinations of them. Doctoring images also involves the pasting one part of an image onto another one, skillfully manipulated so to avoid any suspicion. One effective tool for providing image authenticity and source information is digital watermarking.

These digital watermarks also offer forgery detection. Several watermarking techniques have been proposed. One uses a checksum on the image data which is embedded in the least significant bits of certain pixels. Others add a maximal length linear shift register sequence to the pixel data and identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image. Watermarks can be image dependent, using independent visual channels, or generated by modulating JPEG coefficients. These watermarks are designed to be invisible, or to blend in with natural camera or scanner noise. Visible watermarks also exist. In addition to these, a visually undetectable, robust watermarking scheme has come into existence which can detect the change of a single pixel and can locate where the changes occur. The algorithms work for color images and can accommodate JPEG compression [9].

The embedding of a watermark during the creation of the digital object limits it to applications where the digital object generation mechanisms have built-in watermarking capabilities. Therefore, in the absence of widespread adoption of digital watermarking technology, it is necessary to resort to image forensic techniques. Image forensics can reconstitute the set of processing operations to which the image has been subjected. In turn, these techniques not only enable us to make statements about the origin and authenticity of digital images, but also may give clues as to the nature of the manipulations that have been performed.

One such image forensic scheme is based on the interplay between feature fusion and decision fusion in which three categories of features are considered, namely, the binary similarity measures between the bit planes, the image quality metrics applied to denoised image residuals, and the statistical features obtained from the wavelet decomposition of an image. These forensic features were tested against the background of single manipulations and multiple manipulations, as would actually occur in doctoring images [10].

The availability of powerful digital image processing softwares, such as PhotoShop, XnView, ProShow Gold, makes it relatively easy to create digital forgeries from one or multiple images. Over the past few years the field of digital forensics has emerged to detect various forms of tampering. A common manipulation in tampering with an image is to copy and paste portions of the image to conceal a person or object in the scene.

Another possibility for blind forgery detection is to classify textures that occur in natural images using statistical measures and find discrepancies in those statistics between different portions of the image. At this point, however, it appears that such approaches will produce a large number of missed detections as well as false positives [7].

Another efficient technique which can automatically detect and localize duplicated regions in an image, works by first applying a Principal Component Analysis (PCA) on 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 [11]. This technique is effective on plausible forgeries, and has quantified its sensitivity to JPEG lossy compression and additive noise. The detection is possible even in the presence of significant amounts of corrupting noise.

Building specifically on this work, and more broadly on all of these forensic tools, a new lighting-based digital forensic technique came into existence. While creating a digital composite of two or more people, it is often difficult to match the lighting conditions under which each person was originally photographed and the lighting effects due to directional lighting (e.g., the sun on a clear day). At least one reason for this is that such a manipulation may require the creation or removal of shadows and lighting gradients. To the extent that the direction of the light source can be estimated for different objects / people in an image, lighting inconsistencies can therefore be a useful tool for revealing traces of digital tampering [12].

Also, a newly developed forensic tool came into existence that exploits imperfections in a camera's optical system. When creating a digital forgery, it is sometimes necessary to conceal a part of an image with another part of the image or to move an object from one part of an image to another part of an image. These types of manipulations will lead to inconsistencies in the lateral chromatic aberrations, which can therefore be used as evidence of tampering [13]. This current approach only considers lateral chromatic aberrations. The efficacy of this approach is seen in detecting tampering in synthetic and real images.

As usual, all of these techniques will be vulnerable (weak / defenseless) to countermeasures that can hide traces of tampering. This technique, in conjunction with a growing body of other forensic tools, is effective in exposing digital forgeries.

3. BRIEF MATHEMATICAL REVIEW

The pre-requisite of forgery detection using copy-move algorithm includes – completion of the match process in finite and reasonable time and allowing an approximate match of small image segments. Since any digital image can be considered as an array M x N of pixels with certain associated intensities, any tampering of type copy-move can introduce a correlation between the original image and the pasted one. This correlation can be used to detect the tampering. Primarily there are two approaches used to find the approximate block matching:

1. Exhaustive Search
2. Autocorrelation

Exhaustive Search: In this method, the image and its circularly shifted version are overlaid looking for closely matching image segments. Let us assume that x_{ij} is the pixel value of a grayscale image of size M x N at the position i,j. In the exhaustive search, the following differences are examined:

$| x_{ij} - x_{i+k} \bmod(M)\ j+l \bmod(N) |$, k = 0, 1, …, N-1 for all i and j.

It is easy to see that comparing x_{ij} with its cyclical shift [k, l] is the same as comparing x_{ij} with its cyclical shift [k', l'], where k'=M-k and l'=N-l. Thus, it suffices to inspect only those shifts [k, l] with $l \leq k \leq M/2$, $1 \leq l \leq N/2$, thus cutting the computational complexity by a factor of 4.

Finding the correct threshold value 't' is challenging because even in natural images there may be a large amount of pixel pairs that may produce the differences below the threshold. However, this threshold difference Δx_{ij} can be considered to set the proper threshold value based on the requirements, complexity and results.

The comparison and image processing require the order of MN operations for one shift. Thus, the total computational requirements are proportional to $(MN)^2$.

Autocorrelation: This technique is based on the fact that the original and copied segments will introduce peaks in autocorrelation corresponding to the segments which have been copied and moved. However, the computation of autocorrelation factor after passing the given through High-Pass filter provides better results.

The autocorrelation of the image x of the size M x N is defined by the formula:

$$r_{k,l} = \sum_{i=1}^{M} \sum_{j=1}^{N} x_{i,j}\, x_{i+k,\, j+1},\ i, k = 0, \ldots, M-1,\ j, l = 0, \ldots, N-1.$$

The autocorrelation can be efficiently implemented using the Fourier transform utilizing the fact that $r = x * x'$, where $x_{ij}' = x_{M+1-i,\ N+1-j}$, i = 0… M-1, j = 0… N-1. Thus we have

$r = F^{-1}\{F(x)\, F(x')\}$, where F denotes the Fourier transform.

The working of autocorrelation copy-move forgery detection method is explained in the flowchart below:

that matches exactly two types of methods can be done using following matching techniques.

In case of Block-matching, a minimum segment size is specified this is then considered for the match. To identify the identical rows of the given matrix 'A' are lexicographically ordered. The matching rows are then searched by going through all m x n rows of ordered matrix 'A' and looking for two consecutive rows that are identical.

The blocks form an irregular pattern that closely matches the copied-and-moved foliage. This method also indicates the use of retouch tool on the pasted segment to cover the traces of the forgery.In the Robust match technique, the quantized DCT coefficients are calculated and 'Q' factor is computed that determines the quantization steps for DCT transform coefficients. Since, quantized values of DCT coefficients for each block are compared; the algorithm might find too many matching block pairs.

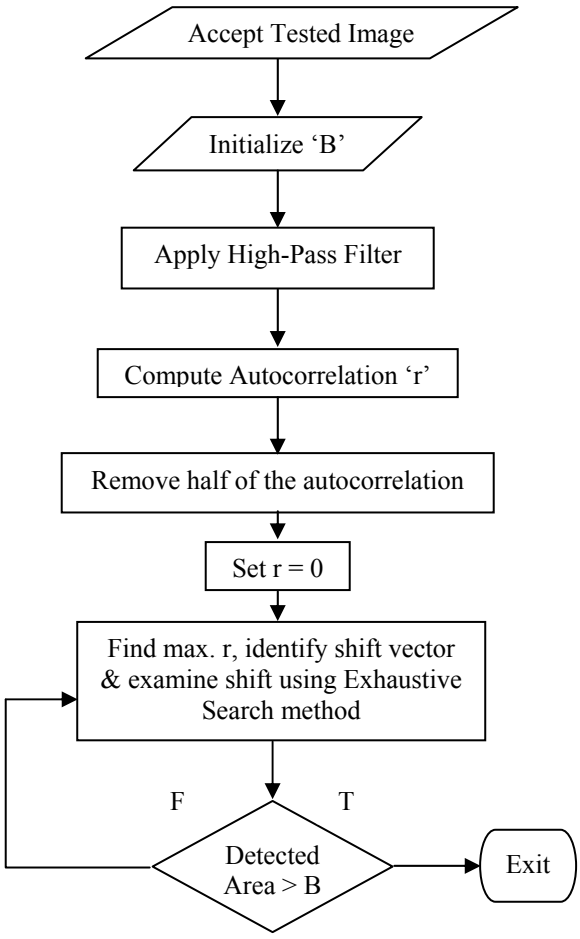

Figure. 2. Flowchart depicting the working of autocorrelation copy-move forgery detection method.

Note: B – Minimal size of a copied-moved segment.
r – Autocorrelation.

This matching can be reduced by computing shift vector 's' between two matching blocks as given below:
$s = (s_1, s_2) = (i_1-j_1, i_2-j_2)$.
Because the shift vectors –s and s correspond to the same shift, the shift vectors s are normalized, if necessary, by multiplying by -1 so that $s_1 \geq 0$.
The Exhaustive search is quite simple and effective and is a most obvious approach whereas the Exact match approach works significantly much better and faster than other approaches. Also, Exhaustive search technique used in detecting copy-move forgery is quite computationally expensive. Moreover, the computational complexity of the exhaustive search makes it impractical for practical use even for medium-sized images.

4. RESULTS AND DISCUSSION

The practice of forging photographs is probably as old as the art of photography itself. Digital photography and powerful image editing softwares like Adobe Photoshop, Xnview, ProShow Gold, made it very easy today to create believable forgeries of digital pictures even for a non-specialist. As digital photography continues to replace its analog counterpart, the need for reliable detection of digitally doctored images is quickly increasing. Recently, several different methods for detecting digital forgeries were proposed. Jessica Fridrich, David Soukal and Jan Lukáš proposed a method based on detection of Copy-Move Forgery in digital images. Also, Alin C Popescu and Hany Farid established a method for exposing digital forgeries by detecting Duplicated Image Regions. Micah K. Johnson and Hany Farid proposed several methods for exposing digital forgeries such as Detecting Inconsistencies in Lighting and detecting inconsistencies through Chromatic Aberration. For each of these methods, there are circumstances when they will fail to detect a forgery. The copy-move detection method is an efficient and reliable detection method which focuses on a special type of digital forgery – the copy-move attacks in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. The method may successfully detect the forged part even when the copied area is enhanced / retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG. This method supports two algorithms for detecting Copy-Move forgery, one that uses an exact match for detection and other that is based on an approximate match. The two approaches introduced by the approximate match algorithm are Exhaustive Search and Autocorrelation whereas two other approaches introduced are Exact match algorithm and Robust match algorithm. The Exhaustive search is quite simple and effective and is a most obvious approach whereas the Exact match approach works significantly much better and faster than other approaches. This method of detection is limited to one particular case of forgeries, when a certain part of the image was copied and pasted somewhere else in the same image (e.g., to cover an object). It is very difficult to use unintentional cameras "fingerprints" related to sensor noise, its color gamut, and / or its dynamic range to discover tampered areas in images. Also, Exhaustive search technique used in detecting copy-move forgery is quite computationally expensive. Moreover, the computational complexity of the exhaustive search makes it impractical for practical use even for medium-sized images. The next method for detecting duplicated regions in an image works by first applying a Principal Component Analysis (PCA) on small fixed-size image blocks to yield a reduced dimension representation that 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. This technique is efficient on plausible / credible digital forgeries and quantifies its robustness and sensitivity to additive noise and lossy JPEG compression. It is such an

efficient technique that automatically detects duplicated regions in a digital image. The detection of duplicated image regions are still possible even in the presence of significant amounts of corrupting noise. This technique works in the complete absence of digital watermarks or signatures offering a complementary approach for image authentication. This representation is robust to minor variations in the image due to additive noise or lossy compression. But still, little doubt is there that counter-measures will be created to foil this technique. The method for exposing digital forgeries by Detecting Inconsistencies in Lighting, for instance, can be a useful / wonderful tool for revealing traces of digital tampering while creating a digital composite of two or more people standing side by side. It is often difficult to exactly match the lighting conditions / effects from the individual photographs due to directional lighting (e.g. the sun on a clear day, floor lamp, single directional light source with controlled lab settings).

This method is efficient in estimating the direction of a point light source from only a single image using various forensic tools adopted from computer vision (field / world). The standard approaches used here for estimating the light source direction / illuminant's direction includes: Infinite Light Source (3-D), Infinite light Source (2-D), Local Light Source (2-D) and Multiple Light Sources. Also, it can be extended to accommodate a local directional light source e.g. a desk lamp, floor lamp. Moreover, it is applicable and effective on both synthetically generated images and natural photographs.

The various loop holes / flaws of this method includes that this solution requires the knowledge of 3-D and 2-D surface normals from at least four and three distinct points respectively on a surface with the same reflectance. With only a single image and no objects of known geometry in the scene, it is unlikely that this will be possible. Manipulations in images in this technique may require the creation or removal of shadows and lighting gradients. Also, this method assumes nearly Lambertian surface for both the forged and original areas and might not work when the object does not have a compatible surface, when pictures of both the original and forged objects were taken under approximately similar lighting conditions. This system also may not work during a cloudy day when no directional light source was present. The Chromatic aberration method is used for automatically estimating lateral chromatic aberration and shows its efficacy in detecting digital tampering. Lateral Chromatic aberration manifests itself, to a first order approximation, as an expansion / contraction of color channels with respect to one another. When tampering with an image, this aberration is often disturbed and fails to be consistent across the image. This approach is effective when the manipulated region is relatively small, allowing for a reliable global estimate. It is efficient for detecting digital tampering in synthetic and real images and can be used to detect tampering in visually plausible forgeries.

This model fails to estimate Longitudinal Chromatic aberrations and other forms of optical distortions. It also fails when the manipulated region is relatively very large. For synthetic images, the average error is 3.4 degrees with 93% of the errors less than 10 degrees. For calibrated / real images, the average error is 20.3 degrees with 96.6% of the errors less than 60 degrees. Thus, the average errors for real images are approximately six times larger than the synthetically generated images. Much of these errors are due to longitudinal chromatic aberrations. Obviously, the problem of detection of digital forgeries is a complex one with no universally applicable solution. Thus, a set of different tools can be all applied to the image at hand. The decision about the content authenticity is then reached by interpreting the results obtained from different approaches. This accumulative evidence may provide a convincing enough argument that each individual method cannot. So in future, all these techniques in conjunction with a growing body of other forensic tools, is effective in exposing digital forgeries. The Comparative analysis of the selected above mentioned algorithms on the basis of the various merits-demerits, domain, types of input-output etc. has been presented in the form of table, Table 1.

5. CONCLUSION

Techniques and methodologies for validating the authenticity of digital images and testing for the presence of tampering and manipulation operations on them have recently attracted attention. Detecting forgery in the digital images is one of the challenges of this exciting digital age. The sophisticated and low-cost tools of the digital age enable the creation and manipulation of digital images without leaving any perceptible traces. As a result, the authenticity of images can't be taken for granted, especially when it comes to legal photographic evidence. Thus, the problem of establishing image authenticity has become more complex with easy availability of digital images and free downloadable image editing softwares leading to diminishing trust in digital photographs. Another common manipulation in tampering with portions of the image is "copy-move". Spotting digital fakes by detecting inconsistencies in lighting is another method. Primarily, in this paper we have reviewed two approaches the Exhaustive Search and the Autocorrelation which are used to find the approximate block matching. Robust search method reduces the number of searches where as exact match search is exhaustive and requires more memory and time. Therefore, robust technique is better in case of time dependent interactive searches.

FUTURE SCOPE

We have been further working on the field of Digital Image Tampering in the following areas:

1. Analyzing other recent algorithms related to forgery detection methods like Digital Watermarking, Inconsistencies in the Complex Lighting Environments, Color Filter Array Interpolation, Re-sampling etc.
2. Video Forgery Detection Methods.

REFERENCES

[1]. I. Pitas - Digital Image Processing Algorithms and Applications; New York: Wiley-Interscience, 2000.

[2]. R. C. Gonzalez and R. E. Woods - Digital Image Processing; New Delhi: Prentice Hall of India Pvt. Ltd., 2005.

[3]. N. F. Johnson and S. Jajodia, "*Exploring Steganography: Seeing the Unseen,"* IEEE Computer, vol.31, no.2, pp. 26-34, 1998.

[4]. A. K. Jain - Fundamentals of Digital Image Processing; New Delhi: Prentice Hall of India Pvt. Ltd., 2001.

[5]. S. W. Smith - The Scientist and Engineer's Guide to Digital Signal Processing; San Diego: California Technical Publishing, 1997.

[6]. A. Riome, Digital Image Forgery Detection Techniques for Still Images. <http://home.wmin.ac.uk/docs/HSCS/andrew2007.ppt>

[7]. J. Fridrich, D. Soukal, and J. Lukáš, *"Detection of Copy-Move Forgery in Digital Images,"* In Proceedings of the Digital Forensic Research Workshop, Cleveland, OH, August 2003.

[8]. *Methods for Detecting Tampering in Digital Images*, Air Force Research Laboratory, August 2000 (AFRL's Information Directorate, Information and Intelligence Exploitation Division, Multi-Sensor Exploitation Branch, Rome, NY).

[9]. R. B. Wolfgang and E. J. Delp, "*A Watermark For Digital Images,"* Proceedings of International Conference on Image Processing, vol.3, pp. 219 – 222, 16-19 Sep 1996.

[10]. S. Bayram, I. Avcıbas, B. Sankur, and Nasir Memon, ***"****Image Manipulation Detection,"* Journal of Electronic Imaging, *SPIE and S&T,* Vol. 15(4), 041102 (Oct-Dec 2006); DOI:10.1117/1.2401138.

[11]. A. C. Popescu and H. Farid, *"Exposing Digital Forgeries by Detecting Duplicated Image Regions,"* Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[12]. M. K. Johnson, and H. Farid, *"Exposing Digital Forgeries by Detecting Inconsistencies in Lighting,"* In ACM. Multimedia and Security Workshop, New York, NY, 2005.

[13]. M. K. Johnson, and H. Farid, *"Exposing Digital Forgeries Through Chromatic Aberration,"* ACM 1595934936/06/0009. MM & Sec'06, September 26–27, 2006, Geneva, Switzerland.

Table 1: Comparison of different Digital Image Forgery Detection Tools / Techniques / Algorithms				
Digital Image Forensic Tools / Techniques / Algorithms	**Works for**	**Domain**	**Merits**	**Demerits**
1. Detecting Lighting Inconsistencies	Effective on both synthetically generated images and natural photographs. Manipulations in images in this technique may require the creation or removal of shadows and lighting gradients.	Efficiently work for Infinite Light Source (3-D), Infinite light Source (2-D), Local Light Source (2-D) and Multiple Light Sources.	This method assumes nearly Lambertian surface for both the forged and original areas and might not work when the object does not have a compatible surface, when pictures of both the original and forged objects were taken under approximately similar lighting conditions.	This system also may not work during a cloudy day when no directional light source is present.
2. Detecting Inconsistencies through Lateral Chromatic Aberrations	Efficient on detecting tampering in visually plausible forgeries.	This approach for detecting tampering is effective when the manipulated region is relatively small.	This approach is efficient for detecting digital tampering in synthetic and real images.	This model fails to estimate Longitudinal Chromatic aberrations and other forms of optical distortions. This approach also fails when the manipulated region is relatively very large.
3. Detection by Classification of Textures in Copy-Move Forgery	Effective on both synthetic and real images.	This method is limited to one particular case of forgeries, when a certain part of the image was copied and pasted somewhere else in the same image (e.g. to cover an object).	Efficient for detecting forgery in small copy areas.	It is very difficult to discover tampered areas in images. Also, Exhaustive search technique used in detecting copy-move forgery is quite computationally expensive.
4. Principal Component Analysis (PCA) in Duplicated Image Regions	Efficient on plausible / credible digital forgeries	An efficient technique that automatically detects duplicated regions in a digital image.	Good for minor variations due to additive noise and lossy compression.	May fail to detect considerable large changes. Little doubt is there that counter-measures will be created to foil this technique