Inspection on the Art of Diverse Image Tampering Approach: A Survey

Sumalatha A
4th Sem, M.Tech
Dept. of CSE
RGIT,Bengaluru

ABSTRACT

Nowadays image authenticity plays a vital role. With the advancement in smartphones and other sophisticated software tools and graphical editors, image tampering detection has become very crucial. Images play a vital role in various fields such as Forensic Investigation, Fashion Industry, Journalism,to gain justice in courtrooms, Tabloid in Magazines etc. This paper reviews all the approaches for various image tampering techniques and provides brief insight knowledge on how these techniques contribute to the detection and tampering.

General Terms

Image authenticity, Image tampering, Image Forensics, EM algorithm

Keywords

Active technology, Passive technology, Digital watermarking, Digital Signature

1. INTRODUCTION

Integrity and authenticity of images is a significant aspect of image forensics and also a rising issue of image processing. The most important task of image forensicsis detection of tampering of images. Due to the advancements in graphics technology, software and hardware tools manipulating images has become very easy with no clues left. Henceforth it is a daunting task to distinguish whether the given image is authentic or tampered.Image forensics deals with obtaining evidence from the documents questioned. Fraud documents are created with ease. In recent years scanners, advanced computers and printing devices are helpful in generating false identity cards, certificates etc. A brief discussion about the various approaches for digital tampering such as active and passive are highlighted along with few methods.

1.1 Applications of Image Forensics

Some of the applications and purpose of image forensics are:

- It is observed for detection of tampered images.
- In various fields such as reducing financial fraud in marketing and business applications, protecting copyright information, journalism, surveillance systems, fashion designing and modeling industries.

1.2 Tampering Approach Classification

Image Tampering detection techniques are classified based on two approaches namely

1. Active Technology
2. Passive Technology

2. ACTIVE TECHNOLOGY

The active technology mainly consists of Data Screening Approach and the Digital Signature Approach. Active technology is mainly motivated by the thought of granting image authenticity generated by digital camera [1,2].

In Data Screening approach a secondary data element like Code authentication is embedded into the image. Hence this approach is also popularly known as intrusive approach [3].

2.1 Active Approach Techniques

2.1.1 Digital Watermarking

This approach is generated at the source end(e.g., camera) and then inserted in the image. The virtue of the watermark is verified at the receiver end. Since the watermarks are inseparable from the image, the watermark has to undergo some transformation as that of the image.

The major drawback is that it must be inserted by the camera device at the time of capturing. It can also be embedded later on with the help of specialized embedding software by an authorized authority. If the image is manipulated the digital watermark is corrupted such that the authenticator can verify its originality [4]. There are various techniques under Digital Watermarking as shown below in Fig 1.

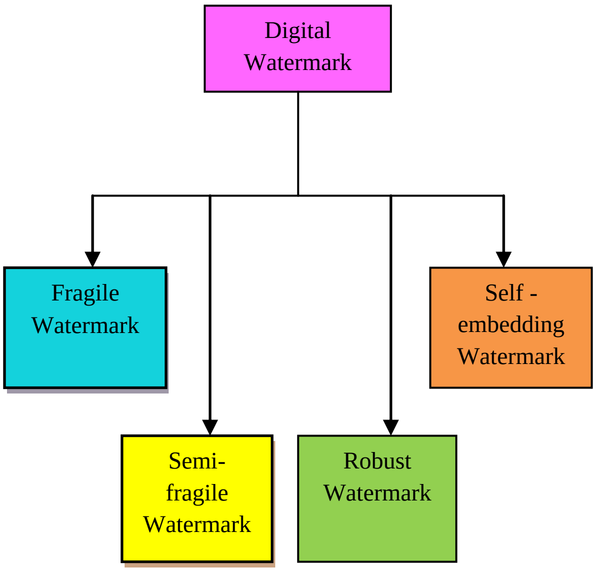


Fig 1: Digital Watermarking Techniques

2.1.1.1 Fragile Watermarks

Fragile Watermarksare built in a manner [5] that a slight manipulation in the image can destroy the watermark. Hence they provide a high probability of tamper detection. The major drawback is that digital images are highly redundant and visual content is generally not modified with minute changes.

2.1.1.2 Semi-fragile Watermarks

Semi-fragile watermarks are moderately robust when compared to fragile watermarks. The major disadvantage is that they are less sensitive to modification in image pixels [6]. Due to this the image can be approved as authentic even when processing operations like JPEG compression of high quality or changing brightness or contrast is applied [7].

2.1.1.3 Robust Watermarks

Robust watermarks are devised to confront any pursuit of destroying the digital watermark. One major aspect of such watermarks is that if image features are inserted or removed which is commensurate in size to the watermarking block, the block consisting of the watermark should be no longer available, depicting tampering in that block. In parallel to this, some of the image processing operations such as lossy compression, gamma correction will evenly affect the image blocks carrying the watermark.Hybrid watermarking is also proposed that are capable of providing key features of fragile and robust watermark [8].

2.1.1.4 Self- embedding Watermark

Self-embedding watermark embed the image into itself. This activates the detection of tampered or cropped image regions and is also useful in recovering the original content or any missing piece of information.

2.1.2 Digital Signature

The Digital Signature approach uses exclusive features extracted from the source image which is later encoded to form a signature[9]. It generates a content-based digital signature which incorporates vital information contents and exclusive producer identification. The signature is generated by a producer-specific private key such that it cannot be tampered. Thereby the authenticator can verify the received image by inspecting whether the contents match the information conveyed in the signature.

An image and signature is generated during the same time. The signature is an encrypted mode of feature codes or hashes of the image and is stored separately[10]. For image authentication the user needs to decrypt the signature and compare the feature codes of the image to their respective values in the original signature. The image can be declared as authentic if they match.

Advantage of Active Approach:

- Computational cost is less and simple if original image is readily available.

Disadvantages of Active Approach:

- Since prior knowledge of original image is needed automatic tampering detection is not achieved.
- Due to the huge availability of digital images in internet without digital signature or watermark. In such cases active approach cannot be validated to find image authenticity [9].
- In Digital Signature approach, an extra bandwidth is needed for signature transmission.

3. PASSIVE TECHNOLOGY

Passive technology was proposed to overcome the problems bumped in the active technology [3]. The techniques used in the passive approach are also called as “passive-blind” methods. Passive technique detects the duplicated objects in tampered image without the original image watermark. There are two methods of passive approach.

1. Identification of source image: This approach identifies the device used for procurement of the digital image. In this method the tampered location in the image cannot be detected.
2. Tampering detection: It detects the willful manipulation of images that aims at modifying the content of the visual image.

3.1 Passive Approach Techniques

3.1.1 Pixel based Technique

Pixel based technique detects the statistical anomalies observed at each pixel level.

3.1.2 Format based Technique

Format based technique leverages the statistical correlations introduced by a lossy compression scheme that is specific.

3.1.3 Camera based Technique

Camera based technique exploits or violates the artifacts introduced by sensors, camera lens etc.

3.1.4 Physically based Technique

Physically based technique explicitly models and detects the anomalies in 3D-interaction between camera, physical objects and light.

3.1.5 Geometric based Technique

Geometric based technique takes object measurements and their positions relative to the camera [11].

Advantage of Passive Approach:

- Already existing digital images and data cannot gain any profit using Active technology. Hence the Passive technology overwhelms this drawback by catering the already existing images.

Disadvantage of Passive Approach:

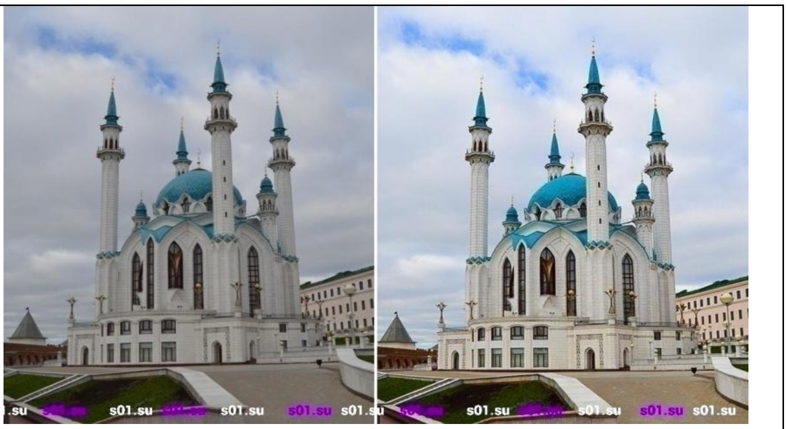
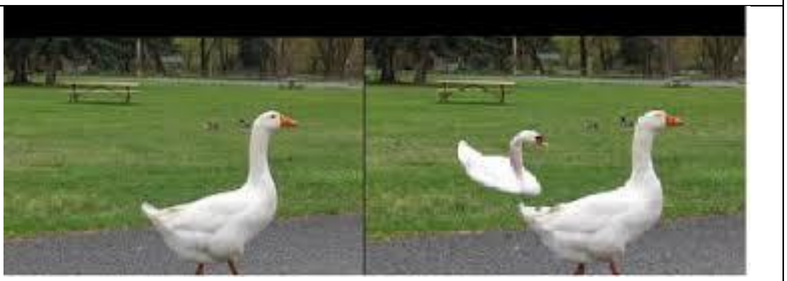
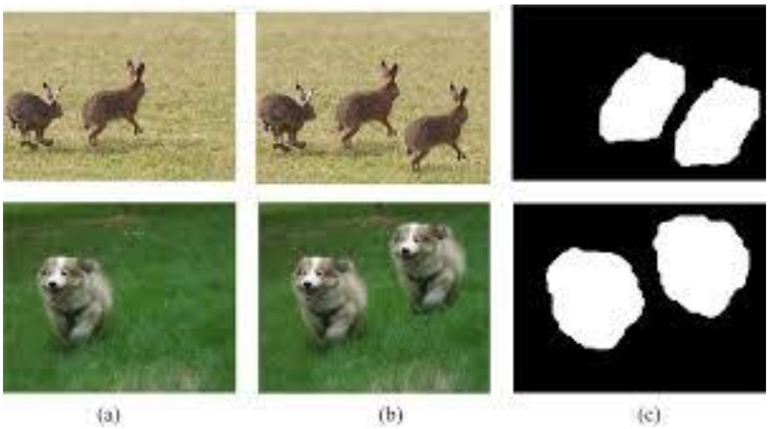
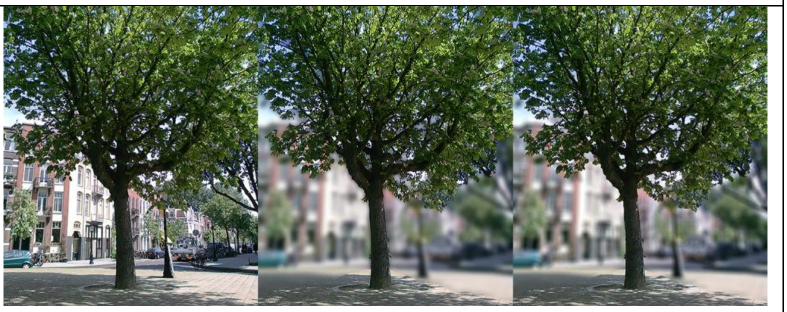
- Passive approach assumes that digital images leave no visual clues that detect tampering and hence need different statistics of an image and thus is complex.

4. TYPES OF DIGITAL IMAGE TAMPERING

The various types of Digital Image Tampering techniques are

1. Image Retouching
2. Image Splicing
3. Copy Move or Cloning
4. Enhanced
5. Morphing

These digital tampering techniques with their pictorial representation and description[12]are depicted inFig.2.

Image Retouching	This method allows the alteration of the image to change the background or fill attractive colors and work with the tint of saturation for balancing and toning [13].	 Original Image Tampered Image
Image Splicing	This method involves composition of two or more images changing the original image significantly to produce a tampered image.	 Original Image Tampered Image
Copy Move or Cloning	In Copy Move part of the image is copied and pasted to another region of the same image [11][15].	 Original Image Tampered Image Tampered Location
Enhanced	The original image is enhanced by color changes or by blurring backgrounds for intended use.	 Original Image Tampered Image

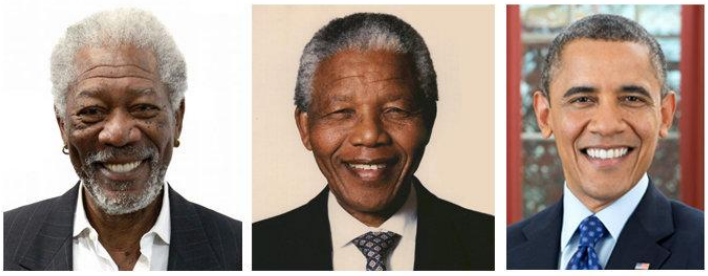
Morphing	This method is used to transfer one person image from another person image to create a new image using transition between two images [14].	 Original Image Tampered Image Original Image

Fig 2: Types of Digital Image Tampering

5. COMPARISON OF IMAGE TAMPERING AND DETECTION TECHNIQUES

Table 1. Techniques for Image Tampering and Detection

Technique for Tampering images	Tools used in Tampering image	Technique for Tampering detection
Block Matching, Exhaustive Search	DCT or PCA	Autocorrelation
Higher order statistics	Crop,rotate,re-sampling,resize	Scale, Stretch, Skew
Bi-coherence, Bi-spectral Analysis	Noise variation estimation	Alpha variance estimation
Copy move	Copy,move	Paste, select
Image Splicing	Copy, resize, move	Paste, select
Expectation and Maximization	EM Algorithm	Compression JPEG, Double JPEG, Encoding JPEG

6. TAMPERING EFFECTS IN DIVERSE FIELDS

The main aim behind tampering is to hide the objects of an image to accomplish gain or to enhance the image for a better outlook.

6.1 Educational Field

Inappropriate information is given to the organization such as fake certificates etc., thereby leading to tampering. This disturbs the management security which is a crucial issue to be solved.

6.2 Medicine Field

Medical images are certified as a proof of poor health and assertion of disease. Medical results are often placed as an evidence for avoiding punishments in courts.Patient reports should be extremely secure and confidential. Also huge amount of money is invested for claiming medical insurance. This leads to the disturbance of the common man security.

6.3 E-commerce Field

Nowadays almost all transactions are carried across the Internet such as online shopping, Bank money transfer which is a threat to the customer's security since there are many unauthorized users and middlemen surfing through the internet. This leads to serious crime and hence is a major issue.

6.4 Fashion Industry Field

Many products in online shopping portals show high quality images of productsthat are unreal and hence betray the customers for their own profits and thus needs to be addressed.

7. BRIEF MATHEMATICAL REVIEW

The imperative concern of tampering detection using copy and move approach incorporates the process of similarity matching in finite and considerable time that allows an approximation match of minute portions of the image. A digital image generally consists of an array of pixels X*Y with certain intensities. Thus upon tampering, the variation of pixel intensity depicts that the image is tampered. This induces a correlation between the original image and the duplicated one. There are two approaches that are used to find the approximate matching of the image segments.

1. Exhaustive Search
2. Autocorrelation

7.1 Exhaustive Search

In this approach, the periodic shifted portion of the image and the image itself are overlaid to search for closely matching portion of the image. Assumption is that m_{ij} is the pixel value of a gray scale image of size X*Y at the position i, j. In Exhaustive Search method, differences of pixel values are computed as,

$$|m_{ij}-m_{i+k}\ \mathrm{mod}(X)\ j+l\ \mathrm{mod}(Y)|$$

where, k=0,1,…..Y-1 for all i and j. When we compare m_{ij} with its periodic shift [k,l] will yield the same results when comparing m_{ij} with its periodic shift [k',l'] where k'=X-k and l'=Y-l. Thus the computational complexity is reduced by a factor of 4 by satisfying for shifts [k,l] with $l \le k \le X/2$, $l \le l \le Y/2$. Calculating the exact threshold value 't' is tedious as there exists a huge amount of pairs of pixels in natural images that may result in variations below the threshold value. The threshold variation Δm_{ij} can be considered to set proper value of threshold depending upon the complexity of results. Comparison of image processing needs the order of XY operations for one shift. Hence the total computational requirements are proportional to $(XY)^2$.

7.2 Autocorrelation

This approach is resulted due to peaks corresponding to image portions that are copied and moved. The autocorrelation computation factor after passing through high pass filter yields better results. The autocorrelation of the image ‘I’ of size X*Y is defined by,

$$r_{k,l}= \sum_{i=1}^{X}\sum_{j=1}^{Y} m_{i,j}, m_{i+k,\, j+l},\ i,k=0,\ldots.X-1,\ j,l=0,\ldots.Y-1$$

The autocorrelation can be implemented using Fourier transform by the fact that r=m*m’, where $m_{ij}'=m_{X+1-i,Y+1-j}$, i=0….X-1, j=0….Y-1. Therefore, $r=F^{-1}\{F(m)F(m')\}$, where F denotes Fourier transform. The working of autocorrelation in copy and move technique is depicted in Fig 3.

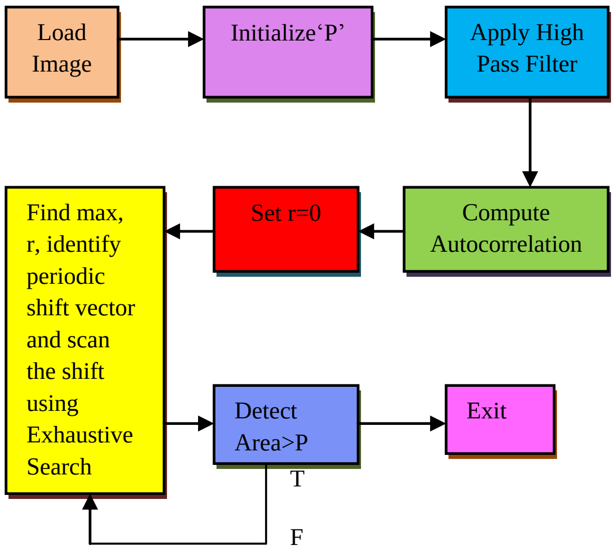


Fig 3: Working of Autocorrelation approach

From the Fig.3 ‘P’ implies the minimum size of the copy and move region. The Exhaustive search is simple but effective. The major drawback is that the Exhaustive Search is computationally expensive. There are two other approaches namely,

1. Exact Match
2. Robust Match

The Exact Match approach works significantly faster than Exhaustive approach. The Exact Match approach limits itself to one case of tampering detection where a portion of the image is copied and pasted in the same image. In Robust Match approach the quantized DCT(Discrete Cosine Transform) coefficients quantization values are calculated for each block and the shift vector can be computed as,

$$s =(s_1,s_2)=(i_1-j_1,i_2-j_2)$$

Since the shift vectors s and –s correspond to same shift they are normalized by multiplying with -1 and hence yield $s_1 \geq 0$.

8. CONCLUSION

In today’s era of digital computing, the need for visual representation has become very essential. Due to the upgrading improvement in networking and computing technologies and high speed bandwidths, images are being manipulated at a faster rate. With the latest smart phones, high end computing devices and sophisticated software and hardware tools manipulating images that leads to tampering has become very easy. The problem of acquiring image authenticity has become more complex with easy availability of digital images and free downloadable photo editors. A brief inspection on diverse techniques has been proposed to identify the tampering in digital images. Tamper detection and recovery is a crucial issue in the field of image forensics and is a current research. Domains like computer graphics, computer vision, machine learning, and signal processing tools have proven to be the best solutions for passive technology detection schemes. The two approaches such as Exhaustive Search and Autocorrelation has been reviewed that depicts matching of the image segments approximately. Also the Robust search method decreases the number of searches whereas exact match search consumes more memory and time. Hence Robust search approach is better in case of dependent interactive searches thereby reducing time complexity.

9. FUTURE SCOPE

Further research studies can be carried out in video tampering detectionthat has become a vital urge in the field of image forensics in this modern era.

10. ACKNOWLEDGEMENT

The author would like to thank the anonymous reviewers for their reviews and comments of future scope in the earlier version of this manuscript.

11. REFERENCES

[1] Friedman, 1993. Trustworthy digital camera: restoring credibility to the photographic image, IEEE Transactions on Consumer Electronics, 39, 4, (1993), 905-910.

[2] Blythe and Fridrich, 2004. Secure digital camera, In Proceedings of the Digital Forensic Research Workshop, (2004), 17-19.

[3] Mahdian B. and Saic S, 2010. A bibliography on blind methods for identifying image forgery, J. Signal Processing: Image Communication, Elseveir, 25, 6, (2010), 389-399.

[4] M.P.Queluz, “Authentication of Digital Images and Video: Generic models and a new contribution” Signal Processing: Image Communication 16(2001), 461-475.

[5] Shan Suthaharan, “Fragile Image Watermarking using a gradient image for improved localization and security”, Pattern Recognition Letters 25(2004) 1893-1903.

[6] Xunzhan Zhua, Anthony T.S. Hob, Pina Marziliano, “ A new semi-fragile image watermarking with robust tampering restoration using irregular sampling”, Signal Processing: Image Communication 22(2007), 512-528.

[7] X. Zhou, X. Duan, And D. Wang, "A Semifragile Watermark Scheme For Image Authentication," In Multimedia Modelling Conference, 2004. Proceedings. 10th International, 2004, Pp. 374-377.

[8] Deguilluame et al.2003. Secure hybrid robust watermarking resistant against tampering and copy attack, J. signal Processing, Elseveir, 83, 10(2003), 2133-2170.

[9] Tzeng and Tsai. 2001. A new technique for authentication of image/video for multimedia applications, In Proceedings of Workshop on Multimedia and Security, ACM Press, new York, USA, (2001), 23-26.

[10] R. Bausvs And A. Kriukovas, "Digital Signature Approach For Image Authentication," Electronics & Electrical Engineering, 2008.

[11] Dr. S.d.Chede, Prof. P.R.Lakhe “Forgery of Copy Move Image Detection Technique by Integrating Block and Feature Based Method” International Journal of Advanced Research in Computer and Communication engineering Vol 4, Issue 1, January 2015.

[12] Hany Farid, “Image Forgery Detection”, IEEE SIGNAL PROCESSING MAGAZINE, pp.16-25, March 2009.

[13] H.Shah, P.Shinde and J.Kukreja, “Retouching Detection and Steganalysis”, IJEIR, Vol.2, pp.487-490, 2013.

[14] M. Sridevi, C. Mala, And S. Sanyam, "Comparative Study Of Image Forgery And Copy-Move Techniques," In Advances In Computer Science, Engineering & Applications, Ed: Springer, 2012, Pp. 715-723.

[15] N. D. Wandji, S. Xingming, And M. F. Kue, "Detection Of Copy-Move Forgery In Digital Images Based On Dct," International Journal Of Computer Science Issues (Ijcsi), Vol. 10, 2013.