Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 3, March 2018, pg.122 – 128

A HYBRID ALGORITHM FOR IMAGE FORGERY DETECTION

Anuradha
M.Tech (CSE)
Beant College of Engineering & Technology, Gurdaspur
anuradha327@gmail.com

Baljinder Singh, Ritika Sood
Assistant Professor, Dept.of Computer Science and Engineering,
Beant College of Engineering & Technology, Gurdaspur
bally648@yahoo.com, ritikasood1987@gmail.com

ABSTRACT: Image forgery detection becomes critical in the current environment since transfer of information now a day is through digital medium. Problem starts to appear as malicious users start to participate over the network. Most common type of forgery in such situation is copy and move. The proposed work uses the application of Gabor filter to detect and prevent copy move forgery and also predict the result in terms of accuracy.
Keywords: Image Forgery, Copy and Move, Gabor Filter, Accuracy.

Introduction

Image processing now days is used widely in order to transfer the data from source towards destination. It may contain additional information hidden by the user within the image. Transfer of images from networked medium may lead to the distortion due to presence of abnormalities. These abnormalities may be due to malicious attacks. These attacks on images that lead to distortion of images are known as forgery. Forgery within the image is a common attack that leads to misleading information. Thus, data at receiver end is not accurate leading to deception.

With the advancement in technology image processing tools and techniques are available for altering the images for forgery. The modification or changes in current image is vital to detect since this image can be used in the authentication process. Image credibility hence required to be verified. This is accomplished by the use of forgery detection mechanism. There are legion of ways by which image can be tempered. For example: resampling, copy and move, splicing etc.

Copy move is not new rather it is an exceptionally old issue.[1] Earlier this is restricted to writing only but with the advancement of technology, this copy move forgery becomes critically part of images. Computerized software is

used greatly for this imitation. Image can be easily changed and controlled by the use of computerised software. It is exceedingly difficult to identify any modification to the existing image.

[2], [3]Image tempering causes loss of information that could be vital to the organization. Falsification is an issue and required to be tackled. For this purpose, forgery detection mechanisms are provided. Procedures are required to be invented to detect the modification to the original image. Image forgery detection is one of the essential issues associated with the forensic science.

The main objective of this paper is to present various image forgery detection procedures; to review some existing and new pixel based image forgery detection mechanisms and to present comparative study of existing procedures used in image forgery detection.

Rest of the paper is organised as follows. Overview of image forgery detection is presented in the first section, in second section image forgery types are discussed, in third section image forgery detection mechanisms are discussed and in forth section literature and comparison of various image forgery detection mechanisms is presented. Last section gives the conclusion of this paper.

1. TYPES OF FORGERY IN IMAGES

Image forgery involves addition of additional pixel or cutting some pixel intensity levels. Deleting some critical features is also objective associated with image forgery. There are distinct methods which are used to forge a digital image. Taking into consideration all of those method, image forgery is divided into following categories.

1.1 Copy Move forgery
1.2 Image Retouching
1.3 Image Splicing
1.4 Image re-sampling

1.1 Copy Move Image Forgery

[4], [5]Copy move forgery mechanism is also known as cloning. Some part of the image is cut in any size and pasted on some other region in this case. Critical information either is lost or replicated in his case. As the copied part originated from the same image hence determining forgery becomes very difficult.

1.2 Image Retouching

This is relatively less impactful forgery mechanism in which image does not alter much. The image features are reduced or enhanced in this case. The contrast or colour of the image is changed but this type of defects is difficult to detect since image alteration is not up to great extents.

1.3 Segment Based Forgery

This is another rarely occurring forgery mechanism within the image. Image is composed of large number of segments or blocks. All of these blocks are sequenced. In this type of forgery, the sequenced blocks are changed to distort the image. Large portion of the image is distorted by the use of this forgery. Segmentation mechanisms are required in ordered to tackle the problem.

1.4 Image Forgery using image Splicing

[4], [6]Image splicing uses cut and paste method form one or more images to create a new image. The new image is also known as fake image. This is one of the most common types of forgery mechanism. This mechanism along with the copy moves forged images are difficult to detect since image intensity levels does not differ much from the original image.

1.5 Image Re-sampling

[7]this is another critical method of image forgery. In this method some part of the image undergoes transformation. Transformation includes translation, rotation, scaling etc. The transformation used in this case could be uniform or

non uniform. Uniform transformation does not alter the shape of the image. The non –uniform transformation on the other hand alter the shape of the image.

The primary focus of study is copy move and image splicing strategies for future enhancements.

2. ANALYSIS OF IMAGE FOREGRY DETECTION MECHANISMS

Image Forgery Detection Mechanisms are critical and are divided into following two categories: active and passive forgery detection.

Active forgery detection mechanism is those in which additional information is packed along with the image for forgery detection. Digital watermarking is an example of it. The problem with this approach is that space requirements associated with forgery detection mechanism enhances greatly. In passive mechanism predefined information is not merged at capturing time and hence consumes much less space as compared to active forgery detection mechanism. Binary patterns are analysed for forgery detection in case of passive forgery detection. Passive image forgery detection is divided into following categories.

2.1 Pixel based Approach

[1]this approach analysis the pixels associated with the given image. Pixel composed of RGB intensity levels. These intensity levels are tempered with in case of forgery. These pixel based approaches are divided into categories including copy move, splicing, re-sampling and statistical. We will focus on copy move and splicing techniques for image forgery detection since they are most commonly used mechanism for forgery detection. Under pixel based approaches following techniques appear

2.1.1 PCA

[8]PCA indicates principal component analysis. This mechanism is used to extract the features associated with the image. The extracted features are selected using the priority analysis mechanism. The features having the priority above the threshold value are selected for examination. PCA reduces the complexity associated with image by reducing the feature analysis by selecting the necessary features only.

2.1.2 DCT

The Discrete Cosine Transform (DCT) calculation is outstanding and regularly utilized for picture pressure. DCT changes over the pixels in a picture, into sets of spatial frequencies. It has been picked in light of the fact that it is the best estimate of the Karhunen_loeve transform that gives the best pressure proportion.[9], [10] The DCT work by isolating pictures into the parts of various frequencies. Amid a stage called Quantization, where parts of pressure really happen, the less vital frequencies are disposed of, henceforth the utilization of the lossy. At that point the most essential frequencies that remain are utilized recover the picture in deterioration process. Subsequently, remade picture is twisted Format Based Approach.

2.1.3 DWT

Wavelet Transform has turned into an essential strategy for picture pressure. Wavelet based coding gives significant change in picture quality at high pressure proportions primarily because of better vitality compaction property of wavelet transforms [8]. Wavelets are functions which permit information investigation of signs or pictures, as indicated by scales or resolutions. The DWT speaks to a picture as a whole of wavelet functions, known as wavelets, with various area and scale. It speaks to the information into an arrangement of high pass (detail) and low passes (estimated) coefficients. The information is gone through arrangement of low pass and high pass channels. The yield of high pass and low pass channels are down inspected by 2.The yield from low pass channel is a rough coefficient and the yield from the high pass channel is a detail coefficient[11], [12]. This method is one dimensional (1-D) DWT. but in this exploration work we are utilizing two dimensional (2-D) DWT. In the event of in two ways, the two lines and sections. The yields are then down examined by 2 toward every path as if there should be an occurrence of 1-D DWT. Yield is gotten in set of four coefficients LL, HL, LH 2-D DWT, the information is gone through arrangement of both low pass and high pass channel and HH.

[13]The image can have the extension such as JPEG, GIF, PNG etc. in case format of the image is analysed for forgery detection than techniques is under the category of format based approach. JPEG image formats are generally used in this approach. Lossy compression causes statistical correlation between the pixels which is analysed using the quantization approach. In case image is compressed then it becomes difficult to detect the forgery through format based approach.

2.1.4 Slant Let Transformation

[14]DWT is generally carried out by the use of filter bank transformation. However this technique cannot be used with time localization. In order to solve the problem time localization based slant-let transformation can be used. This technique is advancement of DWT. At every scale or point of time different filters are used for enhancement of image. Octave band characteristics are retained using this transformation.

2.2 Camera Based approach

[15]As the image is captured from the capturing device such as camera, the image moves from capturing mechanism to memory card or any memory device attached with capturing mechanism. The sensors energy, capacitors and any other electronic circuit may be responsible for loss of information that is tackled using the camera based approach.

2.3 Physical Environment Based Approach

[16]these techniques are based on interaction between physical object, light and the camera. Contrast analysis becomes a key issue in such environment. Contrast differs in case of physical environment analysis. Physical environment based approaches are easy to detect and rarely used to forge the image.

2.4 Geometry Based Approach

[6], [16]in such approaches transformation alter the geometry of the image. The uniformity of the image is disturbed by the application of geometry of the image hence is easy to predict and detect. The detection process is easy hence this approach is also rarely utilized to forge the image.

2.5 Image encryption

This is now days commonly used mechanism in order to detect the forgery within the image. Encryption of image is done in order to perform guard mechanism against the attacks. Parity bits are the commonly used encryption mechanism in which image is encrypted with special bits at particular positions. These positions are specified with power of 2. The formed codeword is transferred at destination end. At destination end decoders are placed in order to decrypt the image. This mechanism is employed in a region of heavy attacks.

Image forgery detection mechanisms are commonly time consuming and hence require certain changes in the current system. Exiting DWT technique is slow due to calculation complexity so in this research, we utilize Gabor filter giving better results in terms of accuracy.

3. PROPOSED SYSTEM

The proposed forgery detection mechanism takes the advantages of Gabor filter to detect any abnormal features fetched from the image. Features are matched against the abnormal feature values. In case abnormality is detected, it is indicated to the user. The proposed methodology is given in terms of flow charts as below.

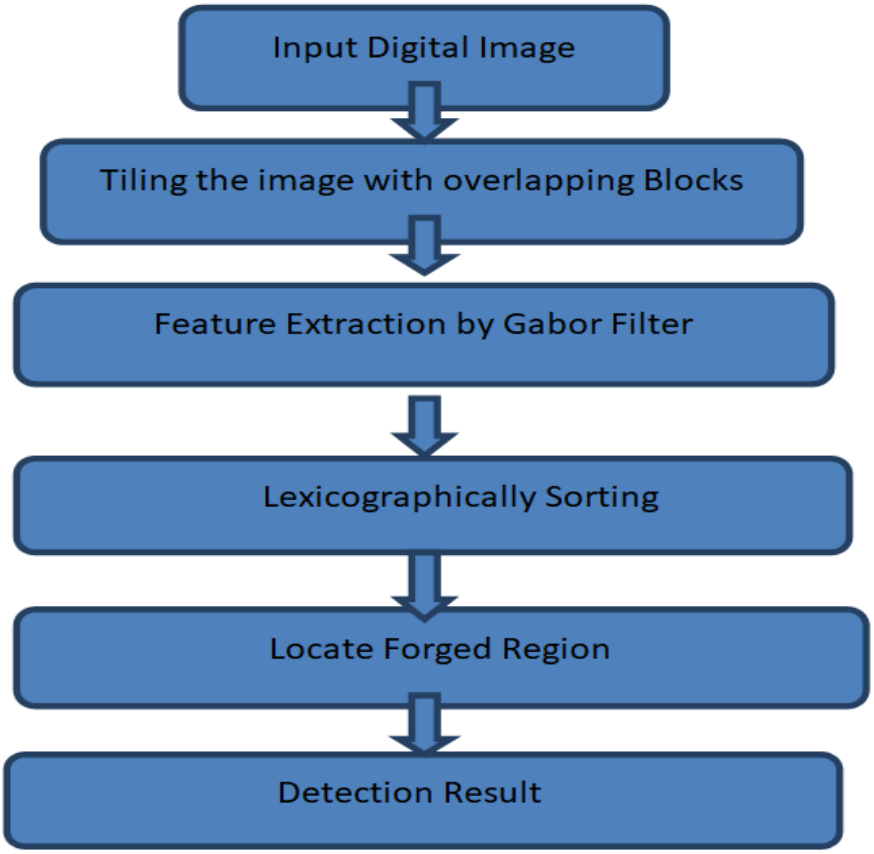


Fig 1: Proposed Methodology1

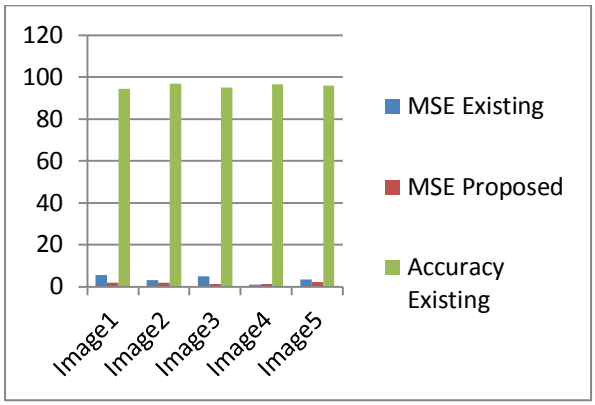
4. Performance Analysis and Results

Performance of the proposed system is judged in terms of accuracy. Value of the actual system is compared against the approximate value and result obtained gives the error. Higher the error, lower will be the accuracy. The result in terms of accuracy is given as below

Image	MSE Existing	MSE Proposed	Accuracy Existing	Accuracy Proposed
Image1	5.4423	2.001	94.4577	97.999
Image2	3.166	1.97	96.8337	98.0246
Image3	4.8328	1.3	95.1672	98.696
Image4	1.02	1.3	96.5095	98.6952
Image5	3.4905	2.1	96.0592	97.8875
Image6	5.1212	1.9	94.8788	98.0778
Image7	5.5423	2.01	94.4577	97.999

Table 1: Plot of MSE and accuracy

Plots of result is given as below



Proposed system accuracy is significantly higher as compared to existing literature. Gabor filter uses iterative approach which produces better result as compared to existing direct approach.

Conclusion

Image tempering causes loss of information that could be vital to the organization. Falsification is an issue and required to be tackled. For this purpose, forgery detection mechanisms are provided. Procedures are required to be invented to detect the modification to the original image. Image forgery detection is one of the essential issues associated with the forensic science. Small or smooth cloned regions are difficult to be detected in image copy-move forgery (CMF) detection. Aiming at this problem, an effective method based on image segmentation and Gabor filer algorithm is proposed. This method segments image into small non overlapping blocks. A calculation of smooth degree is given for each block. Test image is segmented into independent layers according to the smooth degree. Gabor filter is applied in finding the optimal detection parameters for each layer. These parameters are used to detect each layer by hybridization of gabor filter with segmentation based scheme, which can locate a mass of keypoints. The experimental results prove the good performance of the proposed method, which is effective to identify the CMF image with small or smooth cloned region.

REFERENCES

[1] M. D. Ansari, S. P. Ghrera, V. Tyagi, M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-Based Image Forgery Detection : A Review Pixel-Based Image Forgery Detection : A Review," *IETE J. Educ.*, vol. 55, no. 1, pp. 40–46, 2017.

[2] R. V Mahule, "Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain," no. Nckite, pp. 19–26, 2015.

[3] T. K. Das and P. K. Bhunre, "LNCS 8956 - A Secure Image Hashing Technique for Forgery Detection," pp. 335–338, 2015.

[4] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey On Keypoint Based Copy-move Forgery Detection Methods On Image," *Procedia - Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 206–212, 2016.

[5] R. Kaushik, R. Kumar, and J. Mathew, "On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments," vol. 70, pp. 130–136, 2015.

[6] C. S. Gupta, M. T. Scholar, F. Detection, and C. Forgery, "' A Review on Splicing Image Forgery Detection

Techniques ,'" vol. 6, no. 2, pp. 262–271, 2016.

[7] E. E. Kerre, D. Van De Ville, M. Nachtegael, D. Van Der Weken, and E. E. Kerre, "Noise reduction by fuzzy image filtering . IEEE," vol. 125050, no. January 2013, 2003.

[8] M. Mofarreh-bonab, "Image Encryption by PCA," vol. 3, no. 3, pp. 28–30, 2015.

[9] K. Ramani, E. V Prasad, and S. Varadarajan, "Protecting Digital Images Using DTCWT-DCT," pp. 36–44.

[10] A. Sharma, A. K. Singh, and S. P. Ghrera, "Secure Hybrid Robust Watermarking Technique for Medical Images," *Procedia Comput. Sci.*, vol. 70, pp. 778–784, 2015.

[11] M. Imran and A. Ghafoor, "A PCA-DWT-SVD based Color Image Watermarking," pp. 1147–1152, 2012.

[12] S. Rani, "Available Online at www.ijarcs.info Watermarking using DWT and PCA," vol. 6, no. 6, pp. 117–120, 2015.

[13] A. D. Warbhe, "Survey on Pixel and Format Based Image Forgery Detection Techniques," vol. 2012, pp. 7–8, 2012.

[14] N. B. Patil, V. M. Viswanatha, and S. P. M. B, "S LANT T RANSFORMATION A S A T OOL F OR," vol. 2, no. 4, pp. 1–7, 2011.

[15] C. Khare and K. K. Nagwanshi, "Image Restoration Technique with Non Linear Filters," *IEEE*, pp. 1–5, 2011.

[16] R. S. Oommen, "A Survey of Copy-Move Forgery Detection Techniques for Digital Images."

