ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Investigating the Possibility of Recognizing the Forgery by Using Spatial & Transform Domain

Joshi Chintal J[1]
Department of Computer Science Engineering
Parul Institute of Technology
Gujarat, India

Prof. Shailendra K Mishra[2]
Department of Computer Science Engineering
Parul Institute of Technology
Gujarat, India

Abstract: ***This paper reveals basics of Digital (Image) Forensics. A new technology today makes it convenient to quickly, fast, robust, rotation. One of the most successful application digital image forgery detection has recently received significant attention, especially during the past few years. Even though there are many systems to detect the digital image is copied and pasted to another part in the same image. Adaptive regional blend matching method applied for the face detection & tracking of forgery image. ARBM identification of system unknown face & system reporting the determined backup the identify from database of known individual. ARBM verification of system needs to confirm or reject the claimed identified of the real image. DWT-phase correlation and complimenting each other's weakness for effective detection of forgery region from images after that image is divided into overlapping blocks. The performance of the proposed method is demonstrated on several forged images and is proven.***

Keywords: Digital image forensic; Image forgery; Copy-paste forgery detection; Adaptive regional blend matching face detection; Histogram equalization ; DWT; Phase correlation.

I. INTRODUCTION

1.1 Digital Image Forensic : Image Forensics is based on the remark comment observation that any processing carried out during any stage of an image's life cycle whose attending presence can be exploited by forensic analysts to expose the corresponding manipulation. Result as a, high-tech crimes, saleable profitable fraud and other marvels geniuses involve computers. Digital Image Forensics can be subdivided into three branches are:- 1) image source ID; 2) Computer generated image credit praise recognition and 3) Image forgery discovery.

1.2 Image Falsification Detection: Image forgery history has recorded that is happening as early as 1840, Hippolyta banayrd, the first person to create forged image. It is defined as "adding or removing momentous topographies from an image without leaving any obvious traces of forgery". The picture left in Figure 1.1 below is a spectacular image of a "three cyclone" prepared by Hurricane Lilli, which made landfall in Louisiana in early October 2003. However, the same image of the fall 2002 issue of Anchor Lines news letter. The original image was taken in the Gulf of Mexico back in June 2001 by a crewmember of the C-Rambler, a 240-foot supply boat.

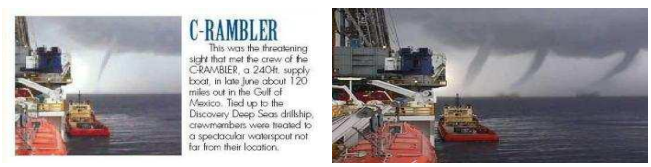


Figure 1.1 Example of C-RAMBLER with a single cyclone in the back (left), forged image with 3 cyclone (right) [18].

There are numerous Types to make forged images, such as:

Spare: Processes that replace some parts of hypermedia content with parts rented from other content. One example is: Replacing a person's face in a photo with one from another photo between two images.

Copy-Paste: Processes that reproduction copies a part of an image and Pasted it into another part of image. For example, in real image some parts are copies and pasted into same another fake image then detect the forged region.

Photomontage: Processes that combine several pictures, creating a new one of high quality.

1.3 Copy- Paste Image Forgery: Copy-Paste forgery detection techniques are used to detect duplicate areas in the original and forged image. Figure 1.2 an example of Seeing Detecting image area forged (a) the original, image, (b) the forged image, (c) the detected regions. A copy-paste fake image is forthright to generate. Figure 1.2 an example of image forgery that seemed in press in July, 2007. The forged image (on the right) shows four Iranian armaments but only three of them are real; two different segments reproduce other image sections by applying a copy-paste attack.

a) Original image b) Forged image

Figure 1.2 an example of image forgery that seemed in press in July, 2007. The forged image (on the right) shows four Iranian armaments but only three of them are real; two different segments reproduce other image sections by applying a copy-paste attack [10].

II. Stimulus and Problem Statement

2.1 Stimulus

Now a day's duplication forgery is the most appropriate method to make fake images. Most of them can only detect those regions which are precisely pasted into another part, but in rehearsal the copied region is climbed or revolved rotated before pasting to attain the best matching with surrounding. We suggest a combinatory method to detect copied region of a forged image. Respectively block resembles to certain types, a number of hauling out as per evocative of blocks for similar through the additional blocks. Next to most recent the cause's are established arranged by the base of complemented blocks allowing for several space thresholds. Here, different other methodologies now block identical. In Transform based method using DWT for blocks are matched. A leading profit of with it is robust vitality compaction material goods are DWT. Improvements are variety of duplicated area, like a noises are totaling and density will be not have emotional impact vitality dimensions.

2.2 Problem Statement

In today's scenario due to advancement of computers and availability of low-cost hardware and software tools it is very effortless to manipulate the digital images without leaving the visible traces of manipulation. It has become difficult to trace these manipulations. As consequences, the integrity and authenticity of digital images is lost. How much can we trust digital images?

III. Proposed Work

3.1 Adaptive Regional Blend Matching (ARBM) Method

Face recognition technology utilizes the ARBM method that provides high speed and high accuracy for facial detection and facial features extraction, which searches and selects face area. The three-dimensional representations of the head are then rotated in both the left-to-right and up-and-down directions. Figure 1.3, ARBM applies differing illumination across the face, which greatly enhanced the chances of a "face print" for matching against its true mate from the database.

Figure 1.3 ARBM method a) original image b) forged image matching the duplicate block [w7].

3.1.1: Face Detection & Track

This is an automatically detect and track a face rotate by any angle and identify face feature matching in figure1.4

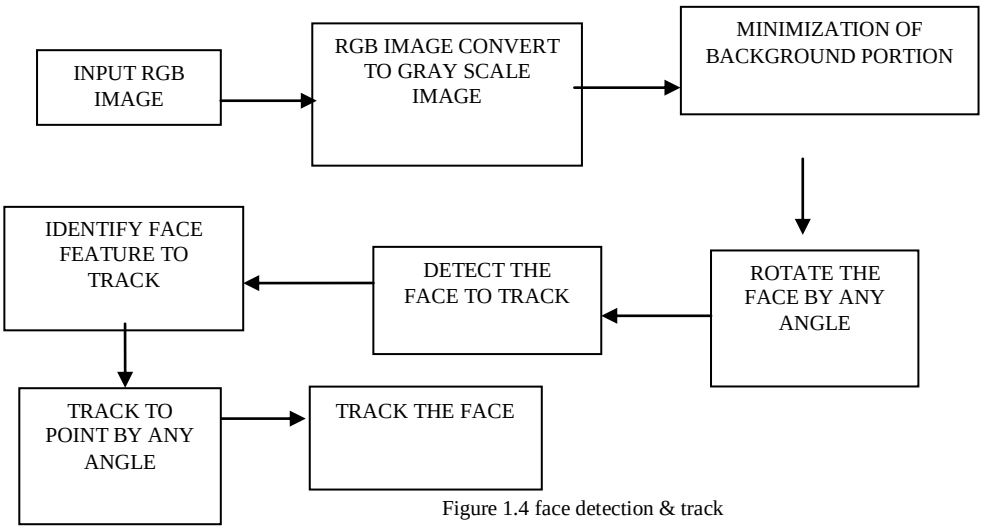
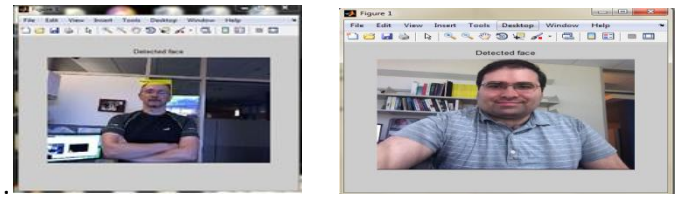


Figure 1.4 face detection & track

In this example, you will develop a simple face tracking system by dividing the tracking problem into three separate problems:

1. Detect a face to track
2. Identify facial features to track
3. Track the face

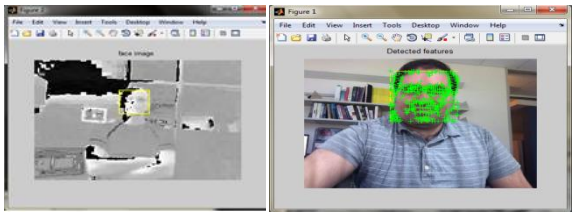
Step 1: Detect a Face to Track: Before you begin tracking a face, you need to first detect it. The ARBM method and a trained classification model for detection. To avoid this issue, and because performing face detection for every face is computationally intensive, and uses a simple facial feature for tracking in figure 1.5 a) & b) detect a face to track



a) b)

Figure 1.5 a) & b) Detect a Face to Track

Step 2: Identify Facial Features to Track: Once the face is located in the face, the next step is to identify a feature that will help you track the face in figure 1.6. Choose a feature that is unique to the object and remains invariant even when the object moves. You can use skin tone as the feature to track. The skin tone provides a good deal of contrast between the face and the background and does not change as the face rotate by any angle in figure 1.7.



a) b)

Figure 1.6 a) & b) Identify Facial Features to Track

Figure 1.7 a) Detect a Rotate Face by any angle

Step 3: Track the Face: With the skin tone selected as the feature to track, you can now use the Histogram Based Tracker for tracking. The histogram based tracker uses which provide the capability to track an object using a histogram of pixel values. Pixels are extracted from the nose region of the detected face. These pixels are used to initialize the histogram for the tracker in figure 1.8. The example tracks the object over successive Face using this histogram.

Figure 1.8 Tracks the Face

3.2 Histogram Equalization Spatial Domain

3.2.1 What is Spatial Domain?

In this image is divided into blocks of size n*n & comparison done on the actual pixel value. Direct manipulation of image pixel. Much faster as compared transform domain.

3.2.2 What is Histogram Equalization?

Image processing of contrast adjustment using the image's histogram. It is a method that improves the contrast in an image, in order to stretch out the intensity range. Image histogram describes how the image pixels are distributed by plotting the number of pixels at each intensity level along with its respective axis. A good image provides Uniform histogram of original image which shows that the image is real image efficiently and secure from any forgery image attacks. It is one kind of best solution to find the between two image original image & forged image. In histogram, it is the graphical representation of the images along with axis. On x-axis each intensity level of image pixels are plotting while on y-axis number of pixels are potted. It is proved that the uniform histogram.

3.2 Transform Domain: It is a Manipulation of transform or wavelet transform of image. It is known as frequency domain. Image is transferred into frequency domain. More computational involved in the process as works with actual pixel value. All the enhancement operation performed on the transform of the image & inverse Transform is performed to get the resultant image. More robustness to common post processing operation. It does work even for image where the attacker has made detection more difficult by applying jpeg quality level changes**.**

3.2.1 Discrete Wavelet Transform: Wavelet decomposition of the images is used due to its inherent multiresolution characteristics [15]. The basic idea of using Discrete Wavelet Transform is to reduce the size of the image at different DWT level. Then the compressed image is divided into overlapping blocks in figure 1.9 a). These blocks are then sorted and duplicated blocks are identified using Phase Correlation as similarity criterion. This approach drastically reduces the time

needed for the detection process and increases accuracy of detection process. Their algorithm is based on pixel matching to locate copy paste regions.

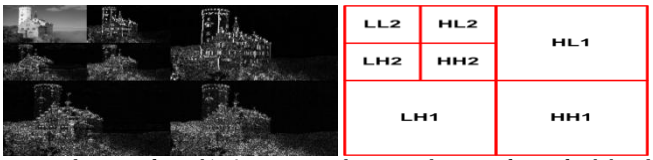


Figure 1.9 a) An image and its Wavelet Transform b) An image and its Wavelet Transform of sub band frequency component [w1].

Sub band LL1 represents the horizontal and vertical low frequency components of the image, Sub band HH1 represents the horizontal and vertical high frequency components of the image, Sub band LH1 represents the horizontal low and vertical high frequency components in figure 1.9 b).

3.3 Algorithm DWT: In the first phase, the exhaustive search for identical blocks is done only on the reduced dimension representation of the image. In the second phase detected blocks of the first phase are compared at different DWT levels. This phase deals with detection of reference and matching blocks on the lowest level of wavelet transform compressed image. This phase deals with checking on different DWT levels to produce more robust output.

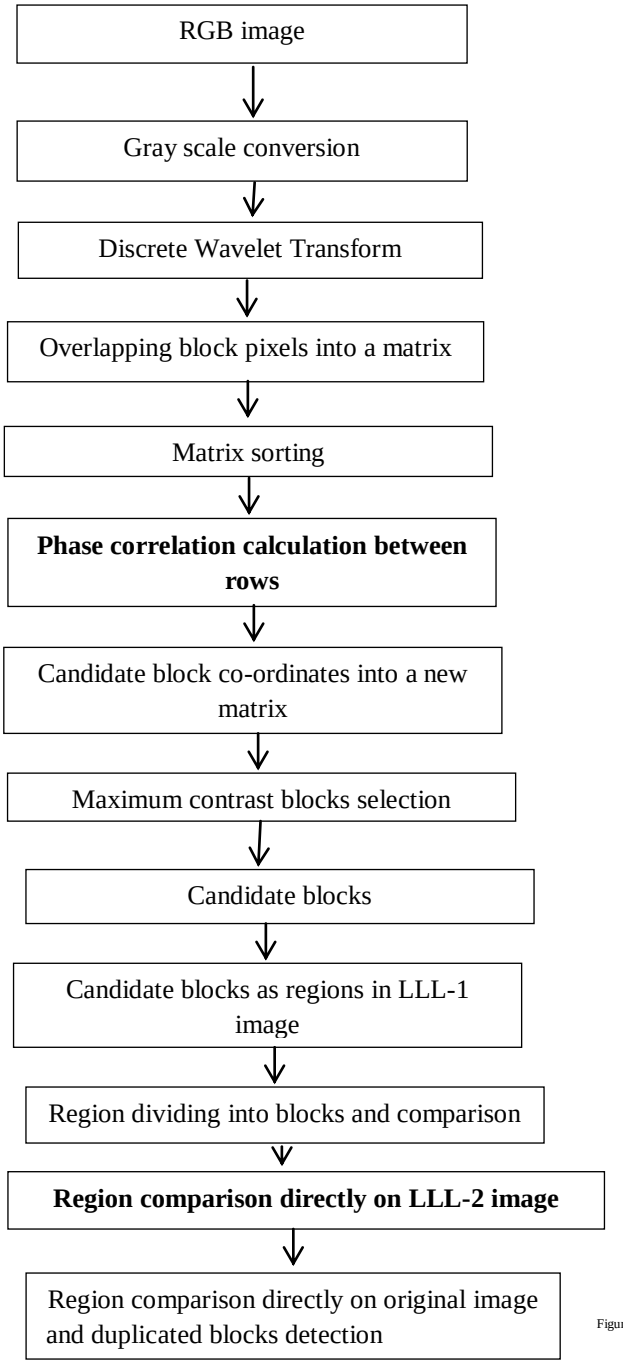


Figure 1.10 Modified Algorithm of Detection & Compare match block

Modified of Phase Correlation: In this Phase correlation of forgery part detection, three levels of decomposition are performed. Overlapping block pixels are calculated. Blocks that have maximum contrast are sorted separately. Phase Correlation done between remaining blocks. Similarly the images at each level of decomposition are subjected to phase correlation. This on repetition and comparison yields the duplicated region. This is an elegant method used for template matching applications. The ratio R between two images 'img1' and 'img2' is calculated as follows:

R = F (img1) ×conj (F (img2))

||F (img1) ×conj (F (img2)) || ----------(1)

where 'F' is the Fourier Transform, and 'conj' is the complex conjugate. The inverse Fourier Transform of 'R' is the phase correlation ρ**.**

Modified Region Comparison Directly on LLL-2 Image is detecting directly duplicate part in image. Due to this, DWTs are used for iterative comparison of matching blocks. If the number of levels used for decomposition is L, then the matching performed on the LL image at level L is denoted by LLL. At each iteration, the images used for matching of overlapping blocks are LLL, LLL-1,…..LL1..LLL image is the image at the lowest resolution. LLL image is used for matching of blocks and then these matched blocks are carried to the next higher level. Final match is performed on the original image itself. H and L denote high and low-pass filters respectively, sub sampling. Outputs of this filter are given by equations (1) and (2). Elements aj are used for next step (scale) of the transform and elements dj, called wavelet coefficients, determine output of the transform. l[n] and h[n] are coefficients of low and high-pas filters respectively One can assume that on scale j+1 there is only half from number of a and d elements on scale j. This causes that DWT can be done until only two aj elements remain in the analyzed signal These elements are called scaling function Coefficients :

$a_j + 1[p] = \sum l\,[n-2p]$ aj [n]……(1)

D_j+1 [p] = ∑ h [n-2p] aj [n]……(2)

3.3.1 Algorithm for Detection and Compare Match Blocks

1. Read the image selected by the user as input.

2. If the input image is not a gray scale image then convert it into a gray scale image.

3. Apply wavelet transform up to specified level to the gray image

4. Each overlapping block pixels into a matrix 4.1 Form a matrix A of dimension b2 columns and (Mb+1) × (N-b+1) rows by extracting the resulting pixel values by rows into a row of A. 4.2 Form another matrix B same as A with two additional columns for storing top-left co-ordinates. 5. Ignore blocks where contrast is minimum.

6. Sort matrix is lexicographically. Then for each row of matrix A

6.1. Compute the phase correlation for the block corresponding to the current row with the blocks corresponding to rows above and below the current row.

6.2. If the computed maximum phase correlation value exceeds a preset threshold value then store the top left coordinates of the corresponding reference block and the matching block from B matrix in a new row of a matrix in . 7. End

8. For LLL-2 level to original image in the image pyramid in figure 3.17 e). For each row of the matrix. 8.1 Form a reference region by padding pixels on all the sides of the b × b reference block. 8.2 Form a matching region by padding pixels on all the sides of the b × b matching block. 8.3. Compare them using Phase Correlation. 8.4. If the computed maximum phase correlation value exceeds a preset threshold value, then store the top left coordinates of the corresponding reference block

and the matching block in a new row of a matrix. 9. End. 10. Plot the blocks as copied and pasted regions on the given image. Then detect the forged region.

IV. Result and Analysis

4.1 Comparative Original Image & its Histogram and Forged Image & its Histogram: Figure 1.11, showing a) Original image name of hello.jpg & its Histogram. Second figure 1.11 b) Editing images which has been detected by the histogram. Forged image name of dup.jpg & its Histogram. Compare of between two image and results are different.

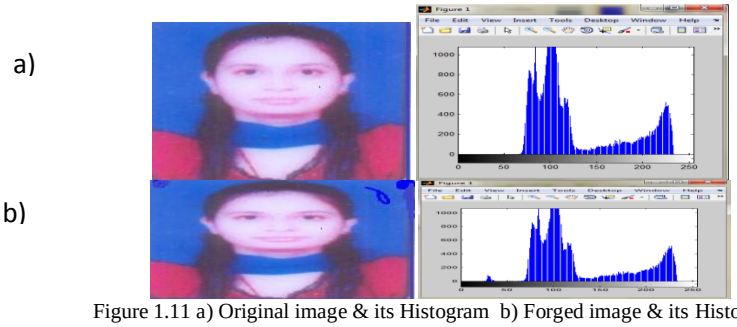


Figure 1.11 a) Original image & its Histogram b) Forged image & its Histogram

Discrete Wavelet Transform: Detect the duplicate region using algorithm of DWT in figure 1.12 and 1.13.

Figure 1.12 a) Original image b) Forged image c) DWT method

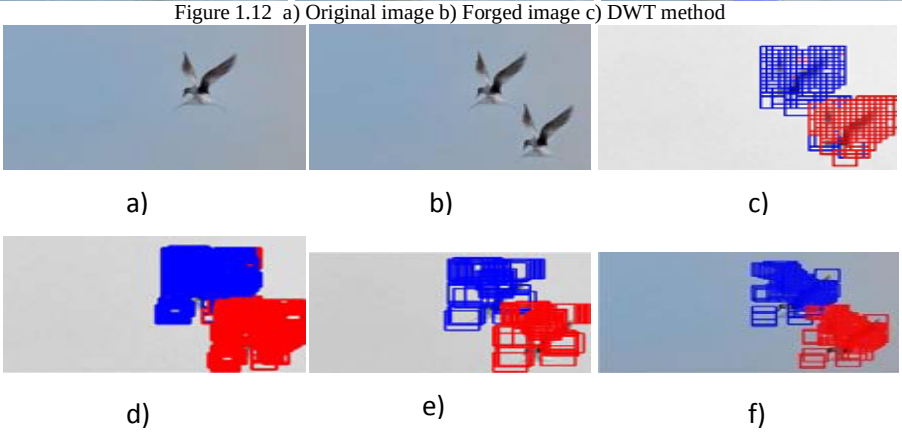


Figure 1.13 a) Original image b) Forged image c) Detection result on LLL level image (d) Detection result on LLL-1 level image (e) Detection result on LLL-2 level image (f) Detection result on forged image

4.2 Comparative Analysis

4.2.1 Comparison of Modified Block based Method & SIFT key point method.

Modified Block based (Proposed Work)	**Existing Work of SIFT key point**
Feature vector matching is used lexicographic sorting	Feature vector matching is not used
Modified Block based method can detect the large transformation	SIFT key point method can not detect the large transformation
Modified Block based method take more memory.	SIFT key point method not take more memory.
Modified Block based method take more accurately detect duplication image	Sift key point method can not much accurately detect duplication

Table 1 difference between Modified Block based & SIFT key point

4.2.2 Compare of PSNR VALUE of image

IMAGE SIZE	PROPOSED METHOD CLAHE (pixel value of image)	BASE PAPER BPDFHE (Pixel value of image)
8*8	10.789	1.098
64*64	21.786	3.564
256*256	25.53	20.64

Table 2 Comparison of PSNR VALUE

V. CONCLUSION AND FUTURE WORK

The developed system has been detecting duplicate region in forgery image using Histogram equalization and DWT block based method. Analysis should prove to be very effective, efficient, fast, robust, quickly and easy to find the how similar two images are confirmed by fake or not. A proposed a method which is more efficient and reliable. Blocks are sorted and duplicated blocks are identified. Adaptive regional blend matching automatically detect, identify face features and track a rotate face by any angle.

In the future, we would like to search for some mechanism to deal with these problems. In addition to this, the same can be extended to work on videos where search for duplicated blocks has to perform on multiple image frames.

References

1. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 9, SEPTEMBER 2014 "Forensic Analysis of SIFT Keypoint Removal and Injection" Andrea Costanzo, Irene Amerini, Roberto Caldelli, Member, IEEE, and Mauro Barni, Fellow, IEEE
2. R. Böhme and M. Kirchner, "Counter-forensics: Attacking image forensics," in Digital Image Forensics, H. T. Sencar and N. Memon, Eds. New York, NY, USA: Springer-Verlag, 2012.
3. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEETrans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.
4. Tampering and Copy-Move Forgery Detection Using Sift FeatureDr.Sivanthi Aditanar College of Engineering,Tiruchendur, Tamilnadu, IndiasInternational Journal of Innovative Research in Computer and Communication Engineering
5. Digital Forensic: Electronic evidence collection, examination & analysis by using combine moments in spatial & transform domain Hani saleh, Sos agaian, Khader mohamd IEEE International conference on system, man & cybernetics(october- 2009)
6. Eric Wharton, Sos Agaian, and Karen Panetta, "A Logarithmic Measureof Image Enhancement," SPIE Defense and Security Symposium, April2006.
7. M. Teague, "Image analysis via the general theory of moments",J.Opt.SocAmer, Vol7O, No 8, pp.920-930, 1980.
8. Whoi-Yul Kim, Yong-Sung Kim, "A region-based shape descriptorusing BP Wavelet Zernike moments" Signal Processing: ImageCommunication, Volume Neural Networks Neural Networks 16, 95-102, 2000.
9. Overview of Existing Techniques of Tamper Detection in Doctored Images Alisha Kamat1 , Pavitra Bhade2 , Rima Paryekar3, Shrutika D. Bordekar., Samarth Borkar Professor, Department of Electronics and Telecommunication Engineering, Goa College of Engineering, Goa, IndiaInternational Journal of Advanced Engineering and Global Technology Vol-1, Issue-4, November 2013
10. Tamper Detection with Reduced Time Complexity Using Hybrid Technique J.Rajalakshmi, K.SureshKumar, A.Vetrikanimozhi Assistant Professor, Department of Electronics and Communication Engineering, CK College of Engineering and Technology, Cuddalore, IFET college of Engineering International Journal of Engineering Science and Innovative Technology (IJESIT)
11. Babak Mahdian1 and Stanislav Saic2,|| Detection of Near-Duplicated Image Regions|| Computer Recognition Systems 2, ASC 45, pp. 187–195, Springer-Verlag Berlin Heidelberg 2007.
12. International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010 "Reduced Time Complexity for Detection of Copy-MoveForgery Using Discrete Wavelet Transform"Saiqa KhanComputer Engineering Dept.,M.H Saboo Siddik College Of Engg.,Mumbai, IndiaArun KulkarniInformation Technology Dept.,Thadomal Shahani Engineering College.,Mumbai, India
13. International Journal of Advanced Engineering and Global Technology Vol-1, Issue-4, November 2013 "Overview of Existing Techniques of Tamper Detection in Doctored Images" Alisha Kamat1 , Pavitra Bhade2 , Rima Paryekar3, Shrutika D. Bordekar4 Department of Electronics and Telecommunication Engineering, Goa College of Engineering, Goa, India.
14. International Journal of Innovative Research in Computer and Communication Engineering"Tampering and Copy-Move Forgery Detection Using Sift Feature" Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamilnadu, India
15. R. Garg, B. Mittal and S. Garg, "Histogram Equalization Techniques for Image Enhancement," International Jour- nal of Electronics and Communication Technology, Vol. 2, No. 1, 2011, pp. 107-111.
16. J. A Stark, "Adaptive Image Contarst Enhancement Using Generalizations of Histogram Equalization," IEEE Tran- sactions on Image Processing, Vol. 9, No. 5, 2000, pp. 889-894. http://dx.doi.org/10.1109/83.841534
17. Y. Gao and M. K. H. Leung, "Face recognition using line edge map," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 6, pp. 764–779, 2002
18. International Journal on Computational Sciences & Applications (IJCSA) Vo2, No.6, December 2012 COMPARISON AND ANALYSIS OF PHOTO IMAGE FORGERY DETECTION TECHNIQUES S.MuraliGovindraj B. Chittapur , Prabhakara H and Basavaraj S. Anami3Mahraja Institute Of Technology, Mysore, INDIA

WEBSITE

19. www.google.com
20. http://www.govtech.com
21. http://www.imageforensic.org/
22. https://www.gov.uk/.../ediscovery-digital-forensic-investigations

AUTHOR(S) PROFILE

Joshi Chintal received the Master of engineering degrees in Computer science & Engineering from Parul Institute of Technology. During 1997-1999, she stayed in vadodara to study of Investigating the possibility of recognizing the forgery by using spatial & transform domain in cyber secyrity.