IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VII (May – Jun. 2015), PP 47-52
www.iosrjournals.org

Passive Image Forensic Method to Detect Resampling Forgery in Digital Images

Amaninder Kaur[1], Sheenam Malhotra[2]
[1,2] *(CSE Department, Sri Guru Granth Sahib World University, India)*

Abstract: *The digital images are becoming important part in the field of information forensics and security, because of the popularity of image editing tools, digital images can be tampered in a very efficient manner without leaving any visual clue. As a consequence, the content of digital images cannot be taken as for granted. Therefore it is must to create forensic techniques which is capable of detecting tampering in image. In general, the image forgery technologies often utilizes the scaling, rotation or skewing operations to tamper some regions in the image, in which the resampling is demanded. Forged area is often resized & rotated to make it proportional with respect to neighboring unforged area. This is called as resampling operation which changes certain characteristics of the pasted portion. By observing the detectable periodic distribution properties generated from the resampling, propose a method based on the Peak Value Identification Classifier to detect the tampered regions and find the Peak Signal to Noise Ratio (PSNR) to know about quality of resampled image. The experimental results show that the proposed method outperforms the conventional methods in terms of recall and precision.*

Keywords: *Digital Image Forensics, Digital Image Forgery, Digital Image Forgery Detection Techniques, K-Nearest Neighbor (KNN), Resampling Detection, Support Vector Machine (SVM).*

I. Introduction

With the tremendous use of digital images and the availability of powerful image editing software's it becomes very important to verify the content of digital images before relying on them. In today's digital world, digital images are one of the principal means of communication. With the advancement and easy availability of image editing tools, it becomes very easy to manipulate or tamper the digital images and create forgeries without leaving any visual clues, and such manipulations may change the whole semantics of the image. The tampered image may totally convey different information than that of the original image. Therefore, digital images have lost their trust and it has become necessary to check the originality of content of the images when they are used in some critical situation like criminal investigation. Hence it becomes very important to verify that whether the image is real or fake. So, the Digital Image Forensics emerged as research field that aims to detect the forgery in digital images. The main goal of digital image forensics is to check the authenticity and integrity of digital images. Digital forgery detection methods can be categorized into following approaches:

1. Active Approach

Active approach requires the pre-embedded information such as watermark or digital signature in digital images for tampering detection. The main drawback of this approach is that it requires pre-embedded information in digital images, which is not always available, because most of the cameras available in the market are not equipped with the facility to embed the watermark or digital signature in images that can be used later in forensic analysis.

2. Passive Approach

Passive approach overcome this drawback and is widely used for forgery detection in digital images as most of the images available today are without any watermark or digital signature. In passive approach different image forgeries are resampling, copy-move (cloning), splicing and retouching. In the work the passive image forensic method is presented to detect one of the important tampering known as Resampling. It is often necessary to resize, rotate, or stretch portions of the images to create a resampled image. This process requires resampling the original image onto a new sampling lattice using some form of interpolation. Resampling introduces specific correlations in the image samples, which can be used as an evidence of editing. Since objects in images are often on different scales, resampling is necessary to create a visually convincing forgery. These operators apply in the pixel domain, affecting the position of samples, so the original image must be resampled to a new sampling lattice. Therefore, by having a reliable technique to detect the resampling forgery will be able to detect forgeries that contain among others this type of tampering. So for the detection of resampling forgery in digital image forensics; a detection technique will be implemented in this work using Peak Value Identification Classifier.

II. Resampling Detection Techniques

In this section, two typical forgery detection methods for the resampling forgery techniques are introduced. These methods detect the forgery by tracing the correlation and interpolation clues of resampled signal.

1. The Popescu's Method

A well known forgery detection method proposed by Popescu [9] assume that the interpolated samples are the linear combination of their neighboring pixels and try to train a set of resampling coefficients to estimate the probability map. In this method, a digital sample can be categorized into two models: M1 and M2. M1 denotes the model that the sample is correlated to their neighbors; while M2 denotes that the sample isn't correlated to its neighbors. The resampling coefficients can be acquired by the EM algorithm. In the E-step, the probability for M1 model for every sample is calculated. In the M-step, the specific correlation coefficients are estimated and updated continuously. The peak ratio of frequency response of the probability map can be used to identify the digital forgery. An SVM classifier was trained to determine if the correlations found by the EM algorithm result from resampling.

2. The Mahdian's Method

Another method proposed by Mahdian and Saic [11] demonstrates that the interpolation operation can exhibit periodicity in their derivative distributions. To emphasize the periodical property, they employ the radon transformation to project the derivatives along a certain orientation. After projecting all the derivatives to one direction the auto covariance function can be used to emphasize the periodicity for detection of resampling forgery. Then, the Fourier transformation computed to identify the periodic peaks. It shows that the resampled image can have strong peaks in the frequency response of the derivative covariance.

III. Proposed Method

In a resampled image certain pixels are linear combination of its neighbors, so find its neighbors in a certain window size of 2N+1 of pixels. Resampled pixels are correlated with its neighbors. This will lead to periodic correlations between resampled pixels. Neighboring pixels can be naturally correlated based on the statistics of the natural image. To detect periodicity, Fourier transform of the probability map is taken. For detection of resampling, the work flow for proposed system is shown in Fig 1.

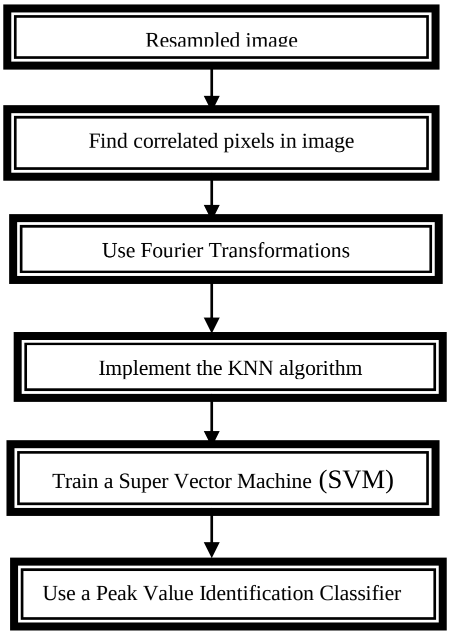

Resampled image
Find correlated pixels in image
Use Fourier Transformations
Implement the KNN algorithm
Train a Super Vector Machine (SVM)
Use a Peak Value Identification Classifier

Fig 1: Work Flow of Proposed System

To find out the periodicity, implement the KNN algorithm and use a Support Vector Machine (SVM) to classify a periodicity map as resampled or nonresampled. The peaks for resampled periodic map are different peak from non-resampled periodic map which are distinguished by classifier.

IV. Results

The proposed method is evaluated on a dataset of personal collected images. These images are also true color which can introduce linear correlations. Resampling imposes periodic correlations between pixels that otherwise do not exist. Below shown Fig 2(a) is original image. Find the KNN of image, which tells about the periodic correlations between resample pixels as shown in the Fig 2 (d); after converting the image into grayscale and black-white image shown in Fig 2 (b) and 2 (c), so that luminance particles can be eliminated from the image. The result of histogram of image is shown below in Fig 2(e).

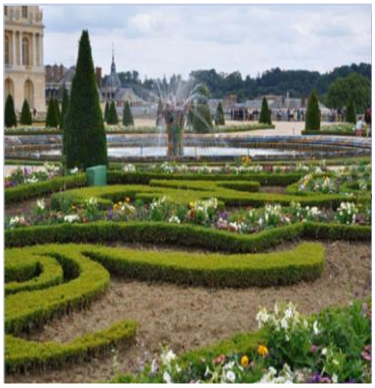


Fig 2 (a): Original Image

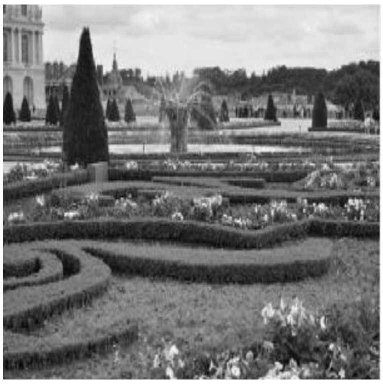


Fig 2 (b): Grayscale Image

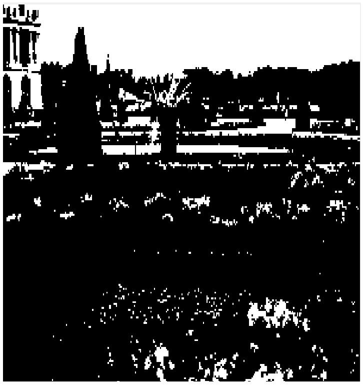


Fig 2 (c): Black-White Image

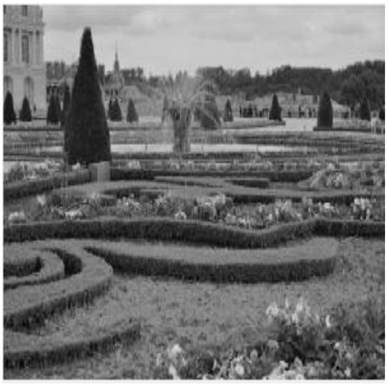


Fig 2 (d): KNN of Image

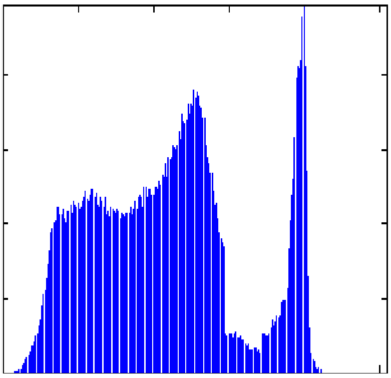


Fig 2 (e): Histogram of Image

For getting the detection part from resampled forged image shown in Fig 3 (a), find the neighbors of pixels. For this categorize the image into 8*8 block size after finding the histogram of image which is shown in Fig 3 (b). So that image will divide into blocks having equaled number of pixels as shown in Fig 3 (c).

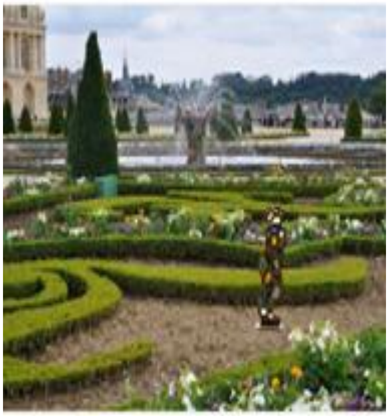


Fig 3 (a): Forged Image

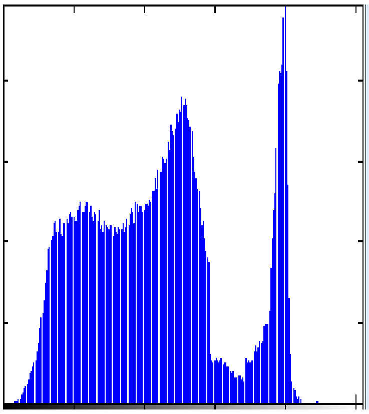


Fig 3 (b): Histogram of Image

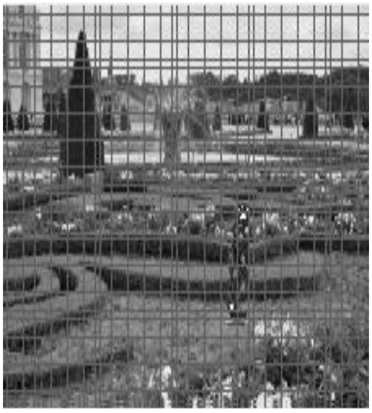


Fig 3 (c): Categorization of Image

To detect the probability of pixels, find FFT (Fast Fourier Transformations) of particular block of resampled image as shown in Fig 3 (d), which tells about the probability of pixels for that particular block shown in Fig 3 (f). Below Fig 3(e) shows the results for FFT of tampered image. After that with the Peak Identification Classifier detects the resampled periodicity map.

Fig 3 (d): Sample Block of Image

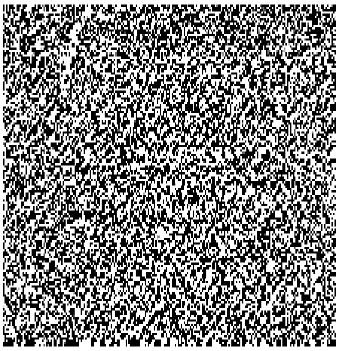


Fig 3 (e): FFT of Image

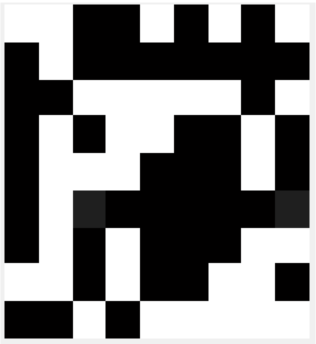


Fig 3 (f): FFT of Sample Block

After detecting the tampered portion in a tampered image, find the probability cluster of 2 and 8 i.e. dimension of statistics, which provides the minimum probability of blocks to show the tampered portion from a resampled image shown in Fig 4 (c) & 4 (e) and find the histogram of that tampered portion shown in Fig 4 (d) & 4 (f) of another original image i.e. Fig 4 (a) & tampered image 4 (b). As compare to probability of Nb=2, in probability cluster of 8 the blocks of tampered part of the resampled image more accurately.

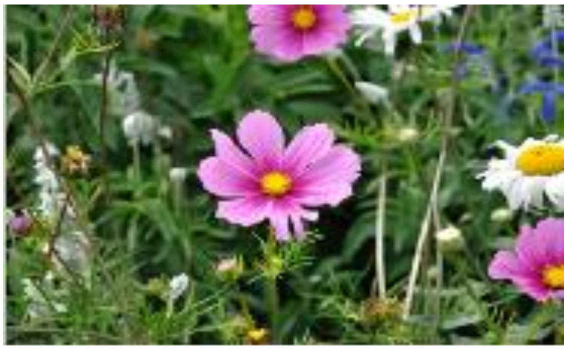


Fig 4 (a): Original Image

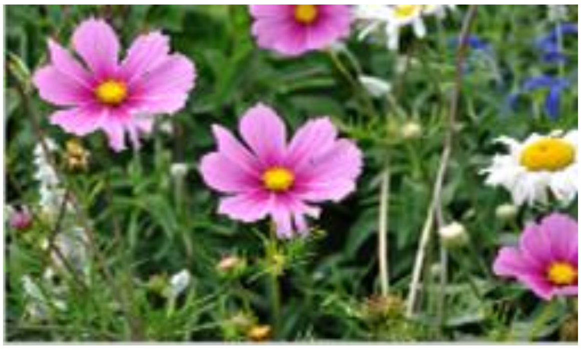


Fig 4 (b): Tampered Image

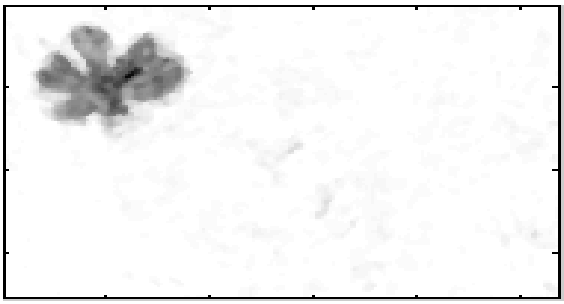


Fig 4 (c): Probability Cluster of Nb = 2

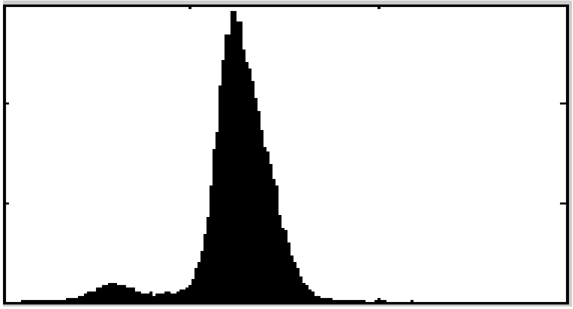


Fig 4 (d): Histogram of Proposed Feature at Nb = 2

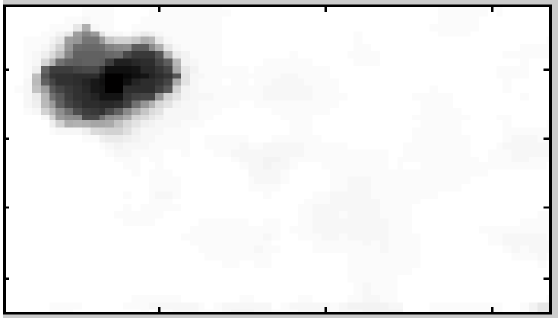


Fig 4 (e): Probability Cluster of Nb = 8

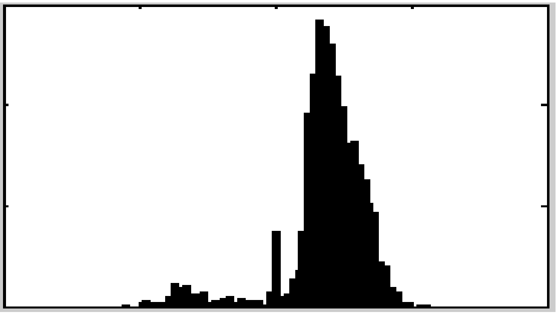
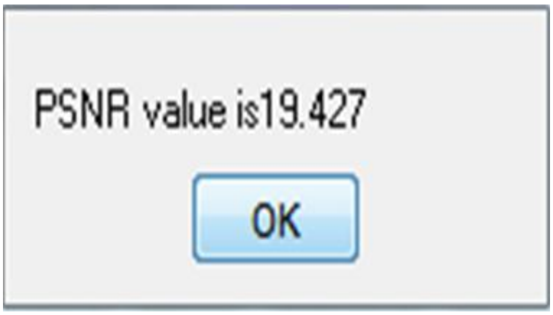


Fig 4 (f): Histogram of Proposed Feature at Nb =8

After getting the results from the resampled image, check the PSNR (Peak Signal to Noise Ratio) to get information about the quality of tampered image which is shown in Fig 5**.** PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.



PSNR value is19.427

Fig 5: Results of PSNR value of Resampled Image

Acceptable PSNR values for quality loss are considered to be about 20 dB to 25 dB. In results the outcome value for PSNR is approximately 20 dB. So the PSNR value for resampled image in the work is acceptable.

V. Performance Measures

To evaluate the robustness and efficiency of the forgery techniques, there are two parameters namely, Precision and Recall rates, which will determine the number of correctly detected tampered parts in an image. As compare to previous research, the window size used is of 128*128 is used, but in these results 8*8 window size is used, which is significantly smaller than 128*128. In the previous results; there is a probability of missing some tampered portion in a resampled image that is of small size than 128*128. So it's not good enough to work with large block size. Smaller blocks size will increase the detection for the correct location of the resampled part in image i.e. used in this work. From the results, the performance of classifier is shown in Table 1.

Table 1: Recall and Precision Rate for SVM Classifier

	Non-Resampled	**Resampled**
Recall (%)	134/135 99.25%	380/390 97.5%
Precision (%)	135/150 90%	380/382 99.74%

The overall recall and precision rates for classifier are shown in Table 1. This classifier performs KNN at low resampling rates. So it gives the more accurate results.

VI. Conclusion

Nowadays, image resampling forgery is becoming a common way the anti-social people are using to create the fake photographs and misusing them. So it is necessary to identify such kind of image manipulations. With the current presented work, it is concluded there are many techniques for detection of resampling forgery in digital image. The current presented work is based on peak value identification classifier. From the results, it is clear that resampling detection with smaller block size of testing sample definitely minimizes the error rate and gives the more accurate results from the previous research in this field. From the results, classifier gives better performance than the KNN classifier. In future, if we will be able to do the resampling detection with lesser block size of testing samples, then it will be definitely gives the more accurate results, but it will take the more space and time for finding the detected parts from the resampled image. So it will be time and space consuming. To overcome this problem in future many other algorithms can be implemented for detection of the resampled part in such a way, so that will take less time and gives the more accurate results. We can also implement the detection algorithms for the other forgeries like copy-move, splicing etc; in digital image forensics.

Acknowledgement

I would like to express a deep sense of gratitude and thanks profusely to God, my Guide Mrs. Sheenam Malhotra, Assistant Professor of Computer Science and Engineering for her valuable advice, suggestions, encouragement and motivation helped me in completing the work in this manner. I also have best regards for Sri Guru Granth Sahib World University, Fatehgarh Sahib, which gives me the opportunity to learn and spread the light of education. I am especially thankful to my parents and brothers, who had always given me the courage, best wishes, support during my career.

References

[1]. P. Sabeena Burvin, P.G. Scholar and J. Monica Esther, “Analysis Of Digital Image Splicing Detection,” IOSR Journal Of Computer Engineering (IOSR-JCE), ISSN: 2278-0661, Vol. 16, pp.: 10-13, Issue No. 2, Ver. Xi, April 2014.

[2]. P. Subathra, A. Baskar and D. Senthil Kumar, “Detecting Image Forgeries Using Re-Sampling By Automatic Region Of Interest (ROI),” Ictact Journal On Image And Video Processing, ISSN: 0976-9102, Vol. 02, pp.: 405-409, Issue No. 04, May 2014.

[3]. P.G. Gomase and N.R. Wankhade “Advanced Image Forgery Detection,” IOSR Journal of Computer Science (IOSR-JCE), ISSN: 2278-8727, pp.: 80-83, April 2014.

[4]. Sanawer Alam and Deepti Ojha, “A Literature Study on Image Forgery,” International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Vol. 2, pp.: 182-190, Issue No.10, October 2014.

[5]. Kusam, Pawanesh Abrol and Devanand, “Digital Tampering Detection,” Bijit - Bvicam’s International Journal of Information Technology and Bharati Vidyapeeth’s Institute Of Computer Applications and Management (BVICAM), ISSN: 0973 – 5658, Vol. 01, pp.: 125-132, Issue No. 2, December 2009.

[6]. A. Meenakshi Sundaram and C. Nandini, “Investigational Study Of Image Forensic Applications, Techniques and Research Directions,” International Journal Of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol. 4, pp.: 636-644, Issue No. 8, August 2014.

[7]. E. Abhitha and V.J Arul Karthick., “Forensic Technique For Detecting Tamper In Digital Image Compression,” International Journal of Advanced Research in Computer And Communication Engineering, Vol. 2, pp.: 1325-1330, Issue No. 3, March 2013.

[8]. A. Popescu and H. Farid, “Exposing Digital Forgeries In Color Filter Array Interpolated Images,” IEEE Transactions On Signal Processing, Vol. 53, pp.: 3948-3959, Issue No. 10, October 2005.

[9]. Alin C Popescu and Hany Farid, “Exposing Digital Forgeries By Detecting Traces Of Resampling,” IEEE Transactions on Signal Processing, ISSN: 1053-587x, Vol. 53, pp: 758 – 767, Issue No. 2, February 2005.

[10]. C. Matthew and K. J. Ray Stamn, Liu, “Forensic Detection Of Image Manipulation using Statistical Intrinsic Fingerprints,” IEEE Transaction on Information Forensics and Security, Vol. 5, pp: 492-506, Issue No. 3, March 2008.

[11]. Babak Mahdian and Stanislav Saic, “Detection of Resampling Supple-Mented with Noise Inconsistencies Analysis for Image Forensics,” International Conference on Computational Sciences and Its Applications, Vol. 8, pp: 546-556, Issue No. 4, 2008.

[12]. V Mire Archana, S. B. Dhok, N J Mistry and P. D. Porey, “Resampling Detection in Digital Images,” International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 84, pp: 24-29, Issue No. 8, December 2013.

[13]. F. Uccheddu, A. De Rosa, A. Piva., and M. Barni., “Detection Of Resampled Images: Performance Analysis And Practical Challenges,” 18th Europeon Signal Processing Conference (Eusipco-2010), Issn: 2076-1465, Vol. 2, pp: 1675-1679, Issue No. August 2014.

[14]. Yan Cheng, “Research on Forensic Identification of Forged Images,” International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), ISSN: 4799-2565, Vol.1, pp: 1152-1155, Issue No.13 December 2013.

[15]. Gupta Pankaj, Singh Jaspal, Arora Anterpreet Kaur and Mahajan Shashi, “Digital Forensics- A Technological Revolution In Forensic,” J Indian Acad Forensic Med., ISSN: 0971-0973, Vol. 33, pp: 166-170, Issue No. 2, June 2011.

[16]. S. Thirumagal and Dr. S. Allwin, “Image Manipulation Detection Using Intrinsic Statistical Fingerprints,” International Journal Of Advanced Research In Computer Science and Software Engineering, ISSN: 2277128x, Vol. 2, pp: 207-212, Issue No. 6, June 2012.

Author Profile

Amaninder Kaur is a student of M.Tech (CSE department), Sri Guru Granth Sahib World University Fatehgarh Sahib, India.

Mrs. Sheenam Malhotra is assistant professor of CSE department, Sri Guru Granth Sahib World University Fatehgarh Sahib, India.