DETECTION OF COPY-MOVE FORGERY USING NORMALIZED CROSS CORRELATION AND FAST FOURIER TRANSFORM

Ms. Apoorva Katyayen, Dr. Ajay Khuteta

Abstract— The authenticity of digital images has become a key concern nowadays because of the easy availability of many image editing tools that made it easier to alter or manipulate any digital image. In the case of forensics, the integrity and authenticity of images are extremely important. So the need for image forgery detection methods has been made obligatory. The proposed forgery detection method in this paper is based on Normalized cross-correlation and Fast Fourier Transform to detect copy-move image forgery. The results show that this method works well to detect those copied image areas that are not detectable with naked eyes.

Keywords—Image Forgery, Copy-Move Forgery, Passive forgery detection, NCC, FFT, SIFT, DyWT, DWT.

I. INTRODUCTION

This era of the digital revolution has made accessing, processing and sharing information effortlessly but at the same time, this technological advancement brought many security challenges too. It's well-known that images are mainly used as a source of information nowadays but the authenticity of this important source has become an issue of concern because of the readily available image editing software like Photoshop, CoralDraw, GIMP, etc. To a large extent, the applications, where digital images are used, are- forensics, medical diagnosis or imaging, entertainment, education, journalism, etc. and these areas are rapidly moving towards being paperless to save the environment and thus force to store data in digital form. For example, if an image is being presented in a courtroom by the victim as evidence then it must be 100% forgery-less in terms to get the true judgment. For this reason, image forensics accepted the challenge of detecting forgery and introduced some robust methods to prevent digital media from illegal forgeries and to secure the authentic data.

To determine the trustworthiness of a digital image, forgery detection can be broadly classified into two categories of Active and Passive forgery detection techniques [1-2]. The active approach authenticates an image by extracting a digital signature and watermark from it. On the contrary, the passive approach has no requirement of any prior information about the image. The passive tamper detection approach is further categorized as 1) Pixel-based techniques; 2) Format-based techniques; 3) Camera-based techniques; 4) Physical-based techniques and;

5) Geometry-based techniques. Among all these, the pixel-based technique further has different types, which are:

- Copy-Move (Cloning)
- Resampling
- Splicing and;
- Retouching

In our research work, we chose to detect copy-move forgery from digital images. Copy-move forgery has an insightful impact on the authenticity of digital images. For this reason, researchers paid much attention to detect this kind of image forgery.

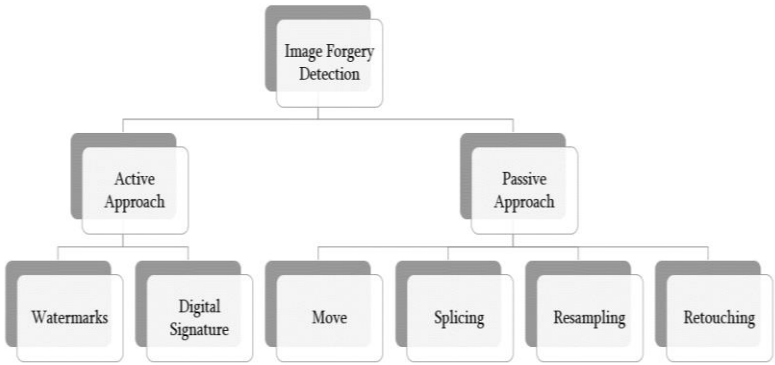

Figure 1: Types of Image Forgery Detection Techniques

Copy-Move or cloning is the most common and the most widely used type of image tampering method, where one needs to cover a part of the image in order to remove or include information that too using a part of the same image. Since finished zones have comparative color, dynamic range, commotion variety properties to that of the image, in image measurable properties it will be unperceivable for a normal human eye researching for contrary qualities. It is said that computational complexity is the key challenge in recognition of copy-move type of forgery because of the extensive search in finding correlated sections. Block matching techniques are used to perceive such counterfeits. Below is a case of copy-move forgery, where the knife in the first image has been copied and pasted at the other part of it to create a forged image as depicted in the second image.

Figure 2: An example of copy-move forgery

II. STUDY OF PRIOR ARTS

We have reviewed many methods of copy-move image forgery detection here. Generally, the forged images are modified by resampling, copy-move, double JPEG, etc. To tamper an image, copy- move is the basic step, which may not achieve enviable results. At times, we use some further processing for the pixels regions such as scaling, boundary smoothing, and rotation.

Investigation of the copy-move forgery and description of an efficient and reliable detection method has been reported. The method successfully detected the forged parts of an image even when the forged image is saved in a lossy format, such as JPEG and when the copied area is retouched or enhanced to merge it with the background. [3]

An efficient technique that is developed that automatically detects forged regions from a digital image. This method works by first applying a principal component analysis to small fixed-size image blocks to yield a compact dimension demonstration. This reduced representation is vigorous to minor variations in the image due to additive noise / lossy compression. Then using lexicographically sorting all of the image blocks, forged regions got detected. [4]

Literature also describes an efficient and robust algorithm for detecting as well as localizing malicious tampering called copy-move. Various forms of post region duplication image processing, including blurring, noise contamination, severe lossy compression, and a mixture of these processing operations used in this technique. [5]. A blind forensics approach based on SVD (singular value decomposition) and DWT (discrete wavelet transform) is also reported. At first, DWT is applied to the image, and SVD is used on fixed-size blocks of low-frequency component in wavelet sub-band to get a reduced dimension illustration. Then the SV vectors are sorted lexicographically and in the sorted list, duplicated image blocks will be close, and

hence will be evaluated during the detection steps. The experimental results show that this approach can decrease computational complexity, and also localize the forged parts correctly even when the image was compressed. [6]

A blind forensics approach to detect copy-move forgery has also been reported. This technique works by applying DWT (Discrete Wavelet Transform) to the input image and the phase correlation is then computed to get the spatial offset between the copied and pasted region. The Copy-Move regions can be now easily found by using pixel-matching, which shifts the input image according to the spatial offset and calculates the difference between the image and its shifted version. [7]

The other technique mentioned works by first extracting SIFTS descriptors of an image, which are invariant to changes in scaling, rotation, illumination, etc. To perceive the similarity between the pasted region and copied region, descriptors are matched with each other to find for any possible forgery in the image. This method efficiently works on noise and lossy JPEG compression, and for compound processing too. [8]

The similar work in this area also illustrates a technique wherein image is first divided into equal sized overlapping blocks, features are then extracted for each block and represented as a vector. Then radix sort is used to sort extracted feature vectors. The difference is computed between the positions of every pair of adjacent feature vectors from the sorting list. The collected number of each of the shift vectors is analyzed. A large accumulated number does mean as the possible presence of a forged region, and thus all the feature vectors corresponding to the shift vectors with large accumulated numbers are detected, whose corresponding blocks are then marked to form a provisional detected outcome. Finally, the connected component analysis and medium filtering are performed on the preliminary detected results to achieve the final result. Here, the radix sort makes the detection more efficient without degrading the detection quality. [9]

Block-matching procedure has also been used earlier authors that first divides the image into the same size block, then improved singular value decomposition is applied to all of the image blocks to yield a compact dimension representation to form the singular value feature matrix of image blocks which are lexicographically sorted. Later, there comes a matching step to find the duplicated blocks based on their feature vectors. Forgery detection decision is made only if the correlation coefficient threshold reached which is set at prior. [10]

An improved algorithm that is based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) to detect such cloning or copy-move forgery. The proposed approach accurately

detects such specific image forgeries as long as the copied region is not scaled or rotated. [11]

A novel forgery image detection scheme for copy-move and splicing forgery image is projected where in, a periodicity analysis is done with the double compression effect in spatial and DCT domain. Feature extraction by SURF descriptors is applied to resist the variation of scaling and rotation. The proposed technique is performed well for the detection of forgery localization. [12]

One of the improved DCT-based method that is developed to detect copy-move forgery. The steps include dividing the image into fixed-size overlapping blocks then apply DCT to each block to signify its features. Truncating is done to reduce the aspects of the features. Feature vectors are then lexicographically sorted and, duplicated image blocks will be adjacent in the sorted list. Then in the matching step, duplicated image blocks will be compared. To make the method more robust, a method is imported to judge whether two feature vectors are the same. Experiment results clearly show that even when an image is manipulated by JPEG compression, blurring or additive white Gaussian noise, this technique is able to detect forgery. [13]

Literature also mentions wherein the original image is first divided into fixed-sized blocks, and then discrete cosine transform (DCT) is applied to each block. Now, each block is represented by the DCT coefficients. In the next step, each cosine transformed block is represented by a circle block and four features are extracted to decrease the dimension of each block. Finally, the feature vectors are sorted in lexicographic order, and duplicated image blocks are matched by a pre-fixed threshold value. Moreover, some parameters are proposed to eliminate the wrong similar blocks. [14]

An effective and computationally efficient method is proposed to detect copy-paste forgery. The proposed forgery detection method is based on the idea of a customized Normalized Cross Correlation (NCC). [15]

Furthermore new key point-based copy-move fabrication location strategy for little smooth districts have been mentioned. Here, the altered picture is portioned into unpredictable and non-covering super pixels, where the super pixels are sorted into the smooth and solid texture. Then, from all super pixels, the steady picture key points are extricated, including smooth, surface and solid surface ones, by using the super pixel substance based versatile component focuses identifier. Now, the nearby visual highlights, exponent moments magnitudes are made for each picture key point, and the best canister first and turned around summed up 2 closest neighbor algorithm are used to discover quickly the coordinating picture key points. Lastly,

the falsely matched picture key points are removed by changing the arbitrary sample consensus, and the copied zones are confined by utilizing zero mean NCC measure. [16]

SIFT qualities are denoted in the identification of picture features and deciding matched focuses. Clustering is the main step which constantly following SIFT coordinating to arrange similar matched points to clusters. The capacity of the picture forensic tool is presented in the evaluation of the transformation that's applied between the two copied pictures of one locale and found them properly. Identifying copy-move forgery is certainly not another methodology but utilizing another clustering approach which has been purposed by utilizing the 2-level clustering technique dependent on spatial and change spaces and any past data about the researched picture or the number of clusters should be made isn't vital.

Almost all these techniques work as depicted in the below figure.

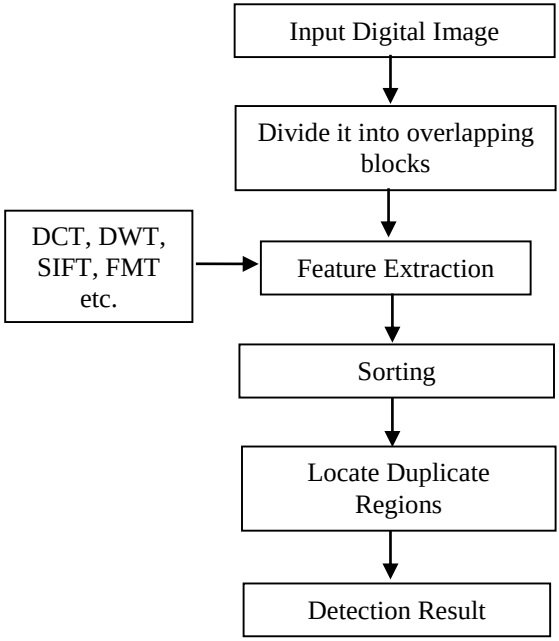

Figure 3: Mostly used process to detect image forgery

There are many ways exist to categorize passive forensic methods on the basis of various points of view. To make the judgment, some features of the images are modeled in different domains.

III. NORMALIZED CROSS-CORRELATION & FOURIER TRANSFORM IN IMAGE PROCESSING

In this work, we targeted to detect copy-move forgery from digital images by using normalized cross-correlation that helps in template matching and pattern recognition in image processing field. Between two images, it makes use of to calculate the level of similarity or dissimilarity between two images or signals. NCC is limited in the range of -1 and 1. NCC can be mathematically given as equation (1):

$$C(x,y) = \frac{\sum_{y'=0}^{h-1}\sum_{x'=0}^{w-1} T(x',y') I(x+x',y+y')}{\sqrt{\sum_{y'=0}^{h-1}\sum_{x'=0}^{w-1} T(x',y')^2 \sum_{y'=0}^{h-1}\sum_{x'=0}^{w-1} I(x+x',y+y')^2}} \quad (1)$$

Where (x', y') are the templates, T, coordinates, (x, y) is the image, I, coordinates, and w and h are the width and height of the template. This analyses pixel-wise cross-correlation and normalize by the square root of the autocorrelation of the pictures. [15]

The properties of the Fourier transform in image processing are image compression, filtering images, enhancement, restoration, reducing blurring and noise, etc. By applying Fourier transform an image gets decayed into its sine and cosine mechanisms. When applying the Fourier transform to an image, we convert it from its spatial domain into a frequency domain or Fourier domain that means that the image now comprehends low frequencies. Exclusion of the irrelevant frequency components compresses the image significantly, without doing much loss in the parts. Because one can concentrate decently on discrete modules of the image now that's why it's much simpler to process.

An image is in the spatial domain primarily i.e. the components of the picture (the RGB components) vary with their strength or we can say intensity in the space (x-axis and y-axis).

Representation =f (x, y).

Fourier transform can be envisioned as a transformation of the image into the spatial domain to another domain called the frequency domain.

Representation = F (u, v)

(u - Frequency change along the x-axis, v-frequency change along the y-axis)

Fast Fourier transform performs correlation which is interrelated to convolution closely. Correlation is used as template matching to locate features of an image. In the image, to view the matching positions of the template, we discover the extreme pixel value and then explain a threshold value that is less than this maximum value. In the resultant image, it is displayed that the locations of these peaks as white spots in the threshold correlation image. In a time-saving context, if direct computation takes time 2^{2n} multiplications then FFT takes $n2^n$ multiplications. So the time saving is $2^n/n$. [16]

IV. PROPOSED ALGORITHM

Our proposed copy-move forgery detection method is based on template matching and uses NCC for this.

The steps of our algorithm are as follows:

Step 1: Let I (x, y) be an input image

Step 1.1: Apply FFT on I (x, y) and convert it to F (u, v)

Step 2: Choose a template T (x, y) from the image I (x, y)

Step 2.1: Apply FFT on template T (x, y) and convert it to T (u, v)

Step 3: For each element and its localized neighbor of F (u, v) and T (u, v)

Step 3.1: Calculate the Normalized Cross Correlation with respect to the image

Step 3.2: If the correlation coefficient is >= 0.96, then store the location as C (u, v)

Step 4: Apply Inverse FFT on C (u, v) and convert it to I* (x, y).

Here, at first, we took a forged image I (x, y) and applied DFT to it F (u, v) to convert it into frequency domain then we chose a template T (x, y) from the image I (x, y). To achieve precision, the template size should always be taken smaller than the image. The smaller the block, the better the precision, but it should not be too small because it takes more time in template processing. Then we applied Fourier transform to this template too to convert it to the frequency domain T (u, v). When

we apply Fourier transform to template or image, NCC can be applied to the image by convolutions.

Fourier transform helps to turn the complex convolution operations into simple multiplications. Next, we find the correlation between the image and this template by overlapping/sliding this block over the image either horizontally or vertically. Normalized cross-correlation returns the correlation coefficient and the location of the template and image. Here, we have set a value of the correlation coefficient, which we call as a threshold value, like 0.96. Above this value, the template is treated as highly matched. If there's a strong correlation existed then the threshold value tends to be 1. The limitation here is that we can't set this value too low or too high as 1 because the threshold value 1 shows the perfect match. For that reason, we choose this value carefully i.e. 0.96 so that the duplicate regions can be perfectly detected and it worked in all our test images.

Thus we can say that the correlation coefficient's value plays an important role in detecting an image's forged regions. The absence of correlation coefficient cannot make the algorithm work. Wherever the correlation is found greater than 0.96, these locations are stored as C (u, v). Now, the inverse DFT has been applied to C (u, v) to get the image back in the spatial domain that we denoted here as I*(x, y).

V. Experimental Observations and Results

The algorithm is tested and implemented in MATLAB R2018a tool. A comparative analysis is presented in terms of computation time and precision rate obtained by changing the template size and with various photo editing tools respectively. In table I, we computed both recall and precision rates that are based on the properly spotted forged portions of the image to analyze the robustness and efficiency. The precision rate (refer equation (2)) is the ratio of appropriately detected image portions and the sum of properly detected parts added to false positives. False positives are those areas of an image which aren't really altered parts but have been detected as forged parts by the algorithm.

$$\textbf{Precision Rate} = \frac{\textbf{Correctly detected parts}}{\textbf{Correctly detected parts+False positives}} * \mathbf{100} \qquad (2)$$

$$\textbf{Recall Rate} = \frac{\textbf{Correctly detected parts}}{\textbf{Correctly detected parts+False negatives}} * \mathbf{100} \qquad (3)$$

TABLE I. Computed value of precision rate and recall rate in various photo editing tools

Test Data	No. of Images	Precision Rate	Recall Rate
Using Paint Tool	50	92.2	92.6
Using Photoshop Tool	50	45.4	37.7
Using Our Approach	50	94.3	93.9

The ratio of properly detected parts to the sum of appropriately detected parts added with false negatives is defined as recall rate (refer equation (3)). Here, false negatives are those regions of an image which have been not revealed by the algorithm but are really forged ones. [17]. Other than calculating computation times with choosing different template sizes of images and computing recall rate & precision rate, we also checked our work in different image formats too.

TABLE II. Detection Techniques and Tested Image Format

Proposed Algorithm	RGB	Gray Scale	JPEG	PNG	BMP
JPEG Block Method	X	X	*	X	X
Direction Filter Method	*	*	*	*	*
Our Technique	*	*	*	*	*
* → Successful positive estimate of tampering					
X → Successful negative estimate of tampering					

Above table shows that our work does well in all kinds of image formats whether it's RGB, grayscale, JPEG, PNG or BMP. Here, some of the pictorial results of forged images are shown after applying the proposed algorithm to it.

We set the threshold value .96 because it performs the finest in terms of computation time and accuracy as well. Also, we analyzed that the best accuracy comes if we take template size smaller but the computation time increases significantly. Thus it's concluded that the template size should be quite larger (but not much larger) so that the computation takes lessen time.

Figure 4: Original Image

Figure 5: Forged Image

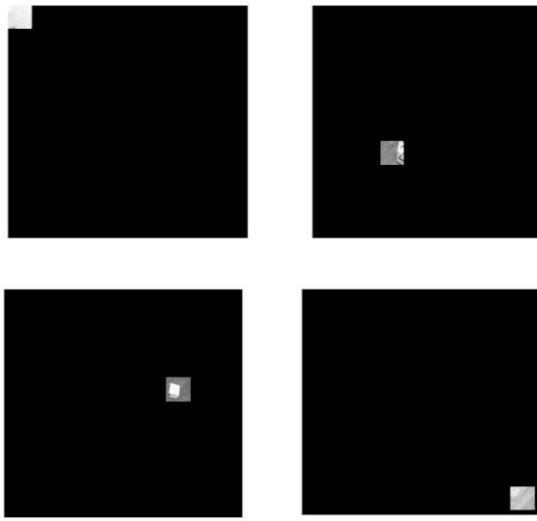

Figure 6: Examples of regions where forgery is not found

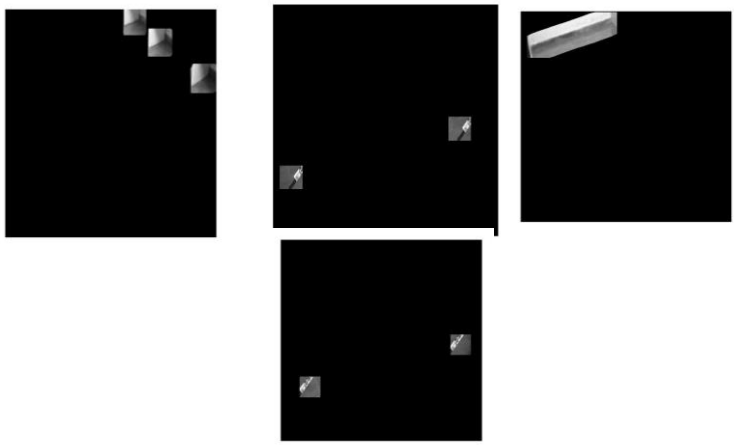

Figure 7: Regions where correlation found (The most possible forged areas)

VI. CONCLUSION

The study shows how the use of NCC and Fast Fourier Transform can help to detect most possible areas of copy-move forgery from an image in less time. In this proposed work, we used various datasets for the study and tested them for different parameters and formats. Different digital image forgery techniques were also discussed which evolved as a result of scientific advancements in the image forensics field. As per table I, we can see that the precision rate is also higher with this work. Also, the results clearly show that the proposed algorithm not only presents the forged areas that are seen easily by human eyes as concluded in the previous works but it also shows the areas that are not easily noticeable. So, if we compare this work with the previously done work, it's clear that the accuracy is significantly increased.

VII. REFERENCES

[1] M. Ali Qureshi, A Review on Copy Move Image Forgery Detection Techniques, 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14).

[2] H-J. Lin, C-W.Wang, and Y-T. Kao. Fast copy-move forgery detection. WSEAS Trans. on Sig. Proc., 5(5):188-197, 2009.

[3] J. Fridrich, D. Soukal, and J. Lukás, "Detection of copy-move forgery in digital images," in Proceedings of the Digital Forensic Research Workshop, Aug. 2003, pp. 5–8.

[4] A. C. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[5] W. Q. Luo, J. W. Huang, and G. P. Qiu, "Robust detection of region-duplication forgery in a digital image," in Proceedings of 18th International Conference on Pattern Recognition (ICPR 2006), Vol. 4, pp. 746–9, 2006.

[6] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, Jul. 2007, pp. 1750–3.

[7] J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting a copy-move forgery in digital images," in IEEE International Conference on Communication Systems, China, 2008, pp. 362–6.

[8] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, Dec. 2008, pp. 272–6.

[9] H.-J. Lin, C.-W. Wang, and Y.-T. Kao, "Fast copy-move forgery detection," in WSEAS Transaction on Signal Processing, 2009, pp. 188–97.

[10] L. Kang, and X.-P. Cheng, "Copy-move forgery detection in the digital image," in 3rd International Congress on Image and Signal Processing (CISP 2010), IEEE Computer Society, 2010, pp. 2419–21.

[11] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2011, pp. 1–4.

[12] S. D. Lin et al., "An integrated technique for splicing and copy-move forgery image detection," in IEEE 4th International Congress on Image and Signal Processing (CISP), Vol. 2, 2011, pp. 1086–90.

[13] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images". Forensic Sci. Int. Vol. 206, pp. 178–84, 2011

[14] Yanjun Cao, T. Gao, and QuntingYang," A robust detection algorithm for copy-move forgery in digital images" Forensic Int. Vol. 214, pp. 33–43, 2012.

[15] Anil Dada Warbhe, R. V. Dharaskar, V. M. Thakare, "Computationally Efficient Digital Image Forensic Method for Image Authentication", in International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015

[16] Wang, XY., Li, S., Liu, YN. "A new keypoint-based copy-move forgery detection for small smooth regions" et al. Multimedia Tools Appl (2017) 76: 23353. https://doi.org/10.1007/s11042-016-4140-5

[17] Abdel-Basset, M., Manoharan, G., Fakhry, A.E., "2-Levels of clustering strategy to detect and locate copy-move forgery in digital images" et al. Multimedia Tools Appl (2018). https://doi.org/10.1007/s11042-018-6266-0

[18] https://www.quora.com/What-is-the-meaning-of-Fourier-transform-of-an-image-Why-is-it-important-in-image-processing

[19] S.Murali, Govindraj B. Chittapur, Prabhakara H. S, Basavaraj S. Anami, "Comparison And Analysis Of Photo Image Forgery Detection Techniques", International Journal on Computational Sciences & Applications (IJCSA) Vo2, No.6, December 2012

AUTHOR'S PROFILE

Ms. Apoorva Katyayen is an M.Tech (Computer Science) student at Poornima College of Engineering, Jaipur. She holds a Bachelor of Technology in Information Technology and her current field of interest is image processing and its applications.

Prof. Dr. Ajay Khuteta is the head of the Computer Science department at Poornima College of Engineering, Jaipur. His area of interest includes Software Engineering, Image Processing, Bio-informatics, etc. He has authored a number of publications in different journals and conferences of national as well as international repute.