International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.9, No.10, (2016), pp.249-258
http://dx.doi.org/10.14257/ijsip.2016.9.10.24

DCT and DWT Based Methods for Detecting Copy-Move Image Forgery: A Review

Anuja Dixit[1], Rahul Dixit[2] and R. K. Gupta[3]

[1,3]*Madhav Institute of Technology & Science, Gwalior, India*
[2]*National Institute of Technology, Rourkela, India*
[1]*anu2010cse1@gmail.com*, [2]*rahul2012ism@gmail.com*, [3]*iiitmrkg@gmail.com*

Abstract

Nowadays, as various image manipulation tools are available very easily. Any person having a little knowledge about these tools can doctor the available images. So digital images are no longer trusted. Computer graphics and digital photography have made the tampering over image easy to commit but hard to detect. Although various image forgery techniques are available but copy-move image forgery is one of the most hard to detect image forgery. In Copy-Move image forgery a segment from the original image is copied and after performing some manipulation over that, segment is pasted at some other location on the same image. This forgery is intended to hide noticeable information shown by the image or for adding information in original image to convey a wrong message. We cannot identify such forgery on the basis of incompatibilities present in an image because the copied segment is taken from the same image so the properties like noise, blur, texture, color palette remain similar to the original image. So, copy-move image forgery is a serious threat to Image forensic Investigators. Researchers have developed several methods for detecting such kind of forgery based on exhaustive search and block based methods. Block based method is more successful in detecting such kind of forgery due to its speed and less complexity. In this paper we discuss forgery detection techniques based on Discrete Cosine Transform and Discrete Wavelet Transform.

Keywords: *Copy-Move, Detection Accuracy, Discrete Cosine Transform, Discrete Wavelet Transform, False Positives, False Negatives, Image compression, Lexicographic sorting*

1. Introduction

It is very well known that Images are better than thousands words. Images can be understood by humans very easily. Images have their various applications. These are used in magazines, newspapers, television, websites *etc.*, Images are used in different fields like medical, crime investigation *etc.*, Due to availability of image processing tools images can be manipulated very easily. Image processing tools like adobe Photoshop, GIMP, Corel draw have the ability to perform tampering over images without any difficulty but such manipulations are very hard to identify. The manipulations done by these tools can be for enhancing an image(innocent editing) and can also be used for conveying a different message through the image which originally was not there in the image *i.e.*, Adding or hiding information conveyed by the image(malicious editing). Alteration made to an image to change its content is known as image forgery. The sole purpose of these forgery could be fun-making, political rivalry, defamation, black-mailing and harassment. So the images are losing their credit and hence they cannot be used as an evidence without checking their authenticity. Digital images have their various applications. As image captures any incidence as it is. These images are very helpful in capturing occurrence of an event. Images describe any situation in a better way than it can be done by millions of words but due to availability of various image processing tools

ISSN: 2005-4254 IJSIP

these images are no longer of trust. They can be easily modified with help of these tools. No extra expertize is required for performing manipulation over an image. Due to such situations which are resulting in distrust in digital images checking the authenticity of digital images is a primary concern. Available images cannot be used without checking their authenticity due to increment in image forgery which is very easy to be done. The forgery involved in images is very hard to identify. For detecting forgeries various forgery detection algorithms are used on the basis of forgery applied in the image. Various kind of forgeries are applied on an image. On the basis of their characteristics they are categorized in different classifications. These image forgery are mainly concerned about manipulating the information reflected by the image. Images could be tampered to delete some information from it. Some alteration in information may take place and also some objects may be added to original image which could be taken from same image or from different images. Image statistics could be changed to enhance the appearance of an image or it could lose its clarity due to addition of noise and blur into it.

(a) (b)

Figure 1. (a) Original Image (b) Tampered Image

Mainly, Image tampering [1] is of three types: Image retouching, Image splicing and copy-move image forgery.

1.1. Image Retouching

Enhancement in an image by adjusting contrast, brightness, noise level and also by edge sharpening and smoothing. In this forgery the sole motive is to provide an image with better visualization.

Figure 2. Image Retouching

1.2. Image Splicing

Original image combined with two or more different images to make a forged image. In this regions from different images are taken to change original image. To identify such kind of forgery the focus is on identifying incompatibilities in image characteristics as regions of different images are used for making forged image.

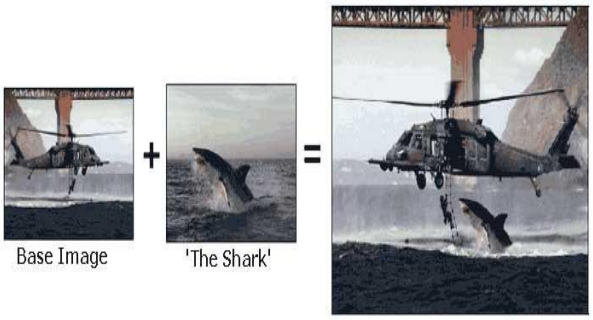

Figure 3. Image Splicing

1.3. Copy-Move Image Forgery

In this forgery a region is copied from the original image then after applying some transformations (like scaling, rotation, stretching, applying JPEG compression, adding noise and blur) region is pasted over the same image at some other location to hide an object in the image or to add some information to change the original message conveyed by the image. Techniques to identify such kind of forgeries is divided in two broad categories.

2. Image Forgery Detection Techniques

Various techniques exist for identifying forgery in an image. On broad level these are divided in two categories. They are active approach and passive approach.

2.1. Active Approach

Digital signatures and Digital watermarking [2] is used. In Digital Signature technique a compressed form of original image is embedded to the host image. These signatures are helpful in identifying if any forgery occur in original image because by doing forgery signature embedded with image will not be changed. Digital watermarking is about embedding a digital copy of the image to itself also known as self-embedding. Only very expensive cameras have this facility to embed watermark in the image when image captured from them. Various cameras does not have the facility to attach watermark with image. A large number of images which are available on the internet do not have watermark attached to them. So this active approach is not very much useful in identifying image forgery.

2.2. Passive Approach

In passive image forgery [3] detection approach no prior information regarding watermark or digital signature is required to detect the authenticity of an image. This approach is focused on identifying forgery in the image based on the image statistics. In passive approach by analyzing input image with help of several operations forgery is identified. Various methods based on DCT and DWT are applied to find forged region in an image. First of all image is divided in overlapping blocks of fixed dimension after that features corresponding to each block is extracted by using wavelet transform and cosine transform. These extracted features are in the form of row vectors. A matrix is formed containing row feature vector corresponding to each block. Further by applying different sorting techniques similar feature vectors are obtained in proximity of each other. Position of each block is stored coordinates used are top left corner point corresponding to each block. On the basis of these coordinates shifting between blocks is calculated. Shift vectors are calculated regarding pair of blocks. Counter value is initialized to zero. Whenever similar shift vector is obtained counter value increased by one. Threshold value

is set for this counter value which help in identifying number of block pairs having similar shifting greater than threshold value. These blocks are identified as forged blocks.

3. Discrete Cosine Transform

DCT (Discrete Cosine Transform) is used for translating spatial domain information into discrete spatial frequency domain. This transform was first used in 1974. At first it was used for image compression which was lossy. Implementation of this method requires less memory and also, for highly correlated images it provides excellent energy compaction. This transform has parallel implementation capability. The ability to produce desired effect of this method is dependent over its ability to present data with help of few coefficients as much as possible.

1-D DCT sequence of length M is given by (1):

$$D(v) = \propto (v) \sum_{y=0}^{M-1} f(x) \cos[\frac{\pi(2y+1)v}{2M}] \quad (1)$$

Where $v = 0,1,2 \ldots\ldots\ldots\ldots, M-1.$

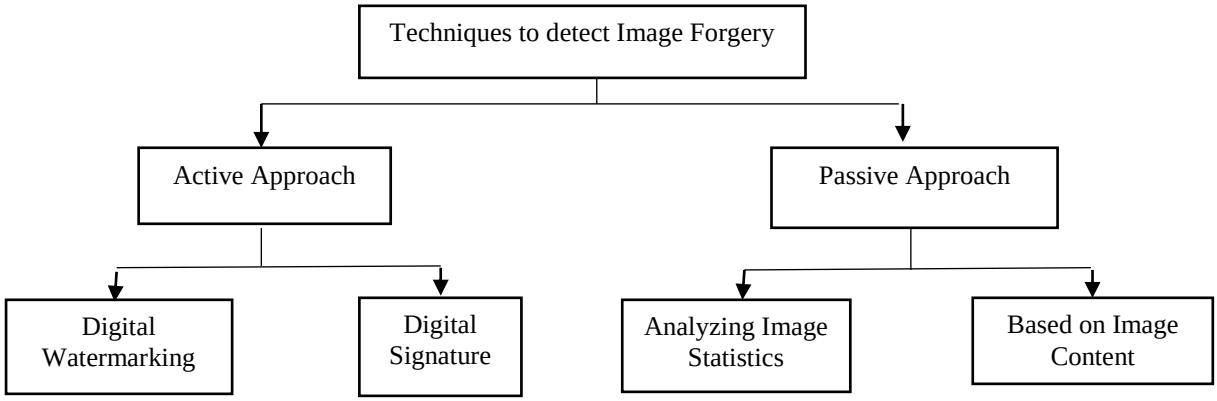

Figure 4. Image Forgery Detection Techniques Categorization

Inverse of transformation is given by (2):

$$f(y) = \sum_{v=0}^{M-1} \propto (v) D(v) \cos[\frac{\pi(2y+1)v}{2M}] \quad (2)$$

Where $y = 0,1,2, \ldots\ldots\ldots M-1.$ and $\propto (v) = \begin{cases} \sqrt{\frac{1}{M}}, & v = 0 \\ \sqrt{\frac{2}{M}}, & v \neq 0 \end{cases}$

4. Discrete Wavelet Transform

Wavelet transformation is utilized for decomposing a signal into a set of basis functions which are known as wavelets [4]. A single prototype is considered which is called mother wavelet $x(s)$ from which wavelets are obtained by using dilation and shifting as in (3).

$$\varphi_{c,d} = \frac{1}{\sqrt{c}} \varphi(\frac{s-d}{c}) \quad (3)$$

Where c is parameter for scaling and d is parameter for shifting.

1-Dimensional wavelet transform is given by (4):

$$W_{f(c,d)} = \int_{-\infty}^{\infty} y(s) \varphi(s) ds \quad (4)$$

4.1. 2-Dimensional Wavelet Transform

DWT [5] has the ability to reduce dimensionality because it possess multi-resolution characteristics. Due to Multi-Resolution it analyzes the different frequencies present in a signal with varying resolution. In 2- dimensional DWT, at each level an image is divided into four subparts. These sub images named as LL, HL, LH and HH. These sub images are also known as sub bands. LL is approximation band. HL contains the horizontal components of an image. LH contains the vertical component of the image. HH is the sub band containing information of diagonal components of an image. These sub bands can be created by applying DWT over input image and also input image can be restored from these sub bands.

5. Related Work

Many researchers have worked over this field and explored various methods for identifying copy-move image forgery in an image. A method based on DCT was proposed by Fridrich *et. al.,* [6]. They suggested two kind of methods. First was based on exhaustive search and other was based on block matching approach. Exhaustive search [7] method for finding forged area was complex method so block based method was developed which is efficient. In this method an image is divided into fixed size block by fixing the size of a sliding window. This slide window moves from top left corner to right bottom corner. Upon each block DCT [8] is applied to extract feature from the block. These feature vectors are stored in a row. Feature vector corresponding to each row are stored in a matrix. Lexicographical sorting is applied on a matrix to identify similar feature vector corresponding to blocks to identify forged areas.

Popescu *et. al.,* [9] proposed a method for detecting copy-move forgery based on Principal Component Analysis (PCA). In this method on each fixed size of block PCA is applied for extracting principle component from a feature vector. After applying PCA Eigen values and Eigen vectors calculated and stored in a row vector. Lexicographical sorting performed so that similar vectors can be in proximity to each other. After that similarity measures are applied to identify similar regions. The advantage of this algorithm is that it can identify forged regions even if copied region I compressed before pasting or noise is added to copied portion. This method is robust against JPEG compression quality level 50.

Hu *et. al.,* [10] proposed a method in which image divided in blocks and after that Discrete Cosine Transform is used for extracting feature vector from it. DCT coefficients are quantized using Quantization table. These DCT coefficients held in a matrix .Lexicographical sorting is performed. In this approach for identifying similar regions Eigen vectors are calculated. This method is efficient and produces less number of false matches hence have high detection accuracy.

Kumar *et. al.,* [11] proposed a fast DCT method. In this method input image divided into fixed sized blocks of dimension 16x16. DCT is applied over each block to extract features of each block of the image. These feature vectors stored in a row vector. Then for enhancing the efficiency and decreasing computation truncating over row feature vector is performed to contain only low frequency component information as these coefficients are rich in information. After truncating row vectors get stored in a matrix. Lexicographical sorting is performed over matrix to arrange vectors such that similar vectors lie in neighborhood. Shift vectors are calculated for identifying blocks having similar sifting. Top left corner coordinates are considered for location identification of a block. A counter is initialized with zero. Whenever similar shift vector is obtained counter value is increased by 1. A threshold value is set and whenever the value of counter which is indication of bunch of blocks having similar shifting is greater than the threshold value that region is labeled with different color to identify copy-move forged region in a digital Image.

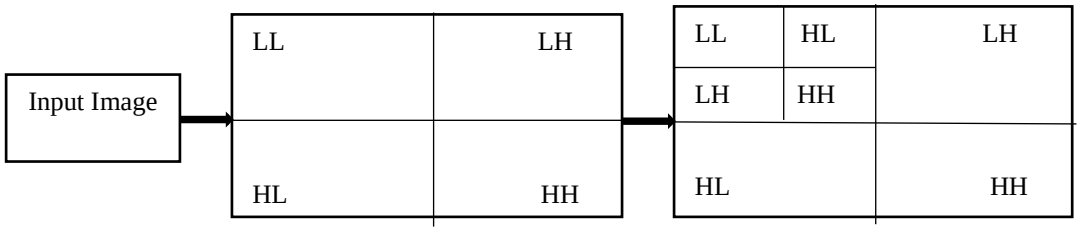

Figure 5. Division of Image Into Sub-Bands Using DWT

Advantage of this method is that it is robust against minor scaling and also if copied region is rotated up to 2^0 before pasting it on the similar image at some other location to hide some information contained in image or for making addition to it. However, the performance of this method is not good in cases where copied moved regions are of small size.

Li *et. al.,* [12] used Discrete Wavelet Transform for finding copy-move image forgery. In this approach input image divided into four sub bands LL, HL, LH, HH which contains the approximation band, Horizontal component of image, Vertical component of image, Diagonal component of image respectively. Only approximation band is considered for further operations applied for identifying forgery in image. In this method approximation band is divided into overlapping blocks. Then for feature extraction singular value decomposition (SVD) is applied for dimensionality reduction. By applying DWT method the complexity involved with finding forged region is reduced to $1/4^{th}$. SVD is responsible for dimensionality reduction of matrix containing feature vector. SVD is useful in dividing matrix in corresponding three components. Two orthogonal matrices are formed from original matrix and one matrix is diagonal matrix which contains singular values as diagonals elements. These singular values are arranged in non-increasing order. These values are used for finding forged region in input image. Advantage of this method is that it is robust against JPEG compression Quality level 70.

Zhang *et. al.,* [13] Proposed a method based on Discrete Wavelet Transform. In this approach DWT is used for dividing image into four sub bands and then using one of them which is called approximation sub band so that complexity for analyzing blocks of image can be decreased. In this algorithm phase correlation is applied to find spatial offset present between copied segment of image and then pasting the same segment after applying manipulation over it at some other location on the same image. This algorithm is robust against several manipulations performed over the copied segment before pasting it but it is very sensitive to shifting performed over copied regions.

Ghorbani *et. al.,* [14] used Discrete Wavelet Transform-Discrete Cosine Transform (Quantized Coefficient Decomposition) for identifying copy-move image forgery detection. In this algorithm at first image is divided in four sub bands. Then approximation band is selected for further processing. DCT is used for feature extraction from the approximation band which is divided into overlapping blocks of fixed size. DCT extracts feature vector from each block. These row feature vectors are stored in a matrix. After that DCT coefficients are decomposed for this quantization is performed using quantized table. Quantized coefficient decomposition is helpful in finding coefficients of lower dimension which result in reduced complexity. Lexicographical sorting is applied over feature vectors. Then shift vectors are calculated corresponding to each pair of blocks. Whenever similar shift vector is obtained between pair of blocks counter value is increased by 1. A threshold value is set when the counter value is greater than threshold then all block pairs having same shift vector is labeled with different color to identify copy move forged region in an image. This method possess high accuracy. The disadvantage with this algorithm is that it cannot identify those copied regions which undergone post processing operations like scaling, rotation, stretching and compression before pasting them to the original image to some other location on the same image.

Zimba *et. al.*, [15] proposed an algorithm based on Discrete Wavelet Transform-Principal Component Analysis (DWT- PCA). In this algorithm firstly, DWT is applied over the image for deducing the image into four sub bands. One of them is called approximation band which is selected for further processing. Approximation band is divided in blocks of fixed dimension.

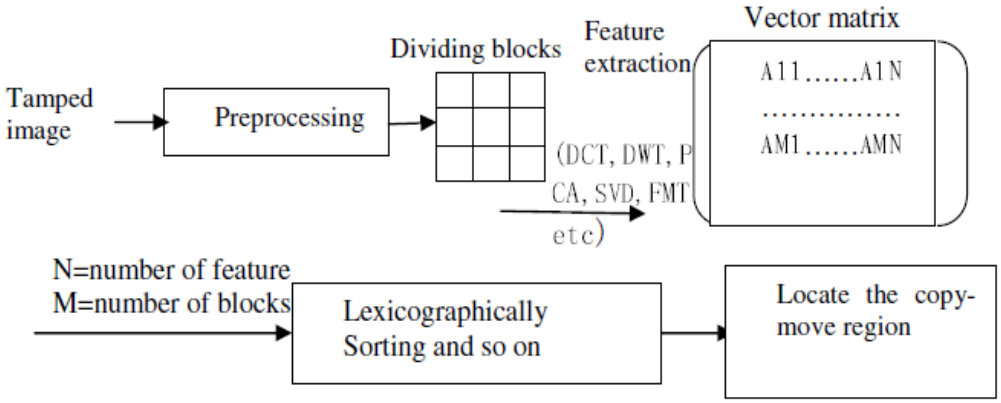

Figure 6. Image Forgery Detection Process

Feature is extracted from these overlapping blocks and stored in matrix. PCA is used for dimensionality reduction of feature vectors. In case of PCA only principle value of feature vectors are considered in such a way that information should not be lost as well as no redundant information should be in feature vector increasing feature vector dimension. Then matrix having reduced dimension feature vectors is lexicographically sorted. After that shift vectors are calculated and normalized to recognize the blocks in an image having similar shifting. This algorithm is able to find out regions which are rotated at varying degrees before pasting them to make a forged image. The disadvantage with this algorithm is that if block size considered for dividing image is greater than the dimension of the forged region in the image then this method will not be able to identify forged copy-move regions in such case.

Zimba *et. al.*, [16] used another approach for identifying forgery. In this algorithm at first Discrete Wavelet Transform is used for dividing image in four sub bands. Lower frequency band also known as approximation band is used. A sliding window of fixed size slide from top left corner to bottom right corner. In this way the approximation band is divided in equal size overlapping blocks. Features vectors are extracted corresponding to each block. These feature vectors are stored in a matrix. Then for arranging feature vector in such a way that similar row factors should be in proximity to each other Radix sort is used. After sorting the similar vectors would be in proximity to each other. Shift vectors are calculated for neighboring blocks. If values of vectors are negative then normalization takes place. Counter value is initialized to zero. If similar shift vector occur between pair of blocks then counter value increased by one. When a certain threshold value is reached for specific shift vector for blocks then theses blocks are labeled with different color to imply the copy-move forged region in an image. Advantage of this method is use of radix sorting in place of lexicographical sorting. Lexicographical sorting has higher complexity than radix sort. The proposed method has less time complexity.

Fattah *et. al.*, [17] proposed a method based on Discrete Wavelet Transform (DWT). Two dimensional DWT is used to find sub bands in an image based on different characteristics. Approximation band which contains low frequency features is used for finding forgery in an image. In this algorithm low frequency band is divided into overlapping and non-overlapping blocks. Candidate blocks are selected from non-overlapping blocks. Similarity found out on the basis of Euclidean distance between

candidate blocks and overlapping blocks. At first it is assumed that the copied region will be pasted at a distance from the location from where it has been copied. For this Euclidean distance is calculated to identify regions situated at some distance for this a threshold value is set. When distance between blocks is greater than the threshold value only then they will be further checked to identify forged region. Once the Euclidean distant constraint is crossed after that Shift vector between blocks is calculated to identify blocks will similar shifting. These blocks shown in different colors and represents the copy-move forged blocks. The proposed algorithm results in reducing huge computational overhead. This method attains higher detection accuracy due to less occurrence of false positives and false negatives.

6. Conclusion

In this paper we have presented a review on techniques based on DCT and DWT for identifying forged region in an image resulted due to copy-move image forgery. Several algorithms are suggested by different researchers using DCT and DWT for detecting copy-move forged region of an image. These methods have their different pros and cons. The detection accuracy of these methods vary on the basis of transformation applied on the copied region as scaling, rotation or some other post-processing operations. Several operations are there which performed after pasting copied region such as noise addition, blurring. Some operations like JPEG compression at different quality levels are applied over the image which are hard to detect forgeries. The detection results also varies based on the size of forgery present in an image, size of blocks considered for sliding window, type of sorting technique applied to sort feature vectors stored in a matrix or the measures taken for identifying shifting between blocks. There is lot of scope in this field for research to discover such techniques which could be robust against several forged operations simultaneously.

References

[1] M. Ali Quereshi and M. Deriche, "A review on copy move image forgery detection techniques", IEEE, **(2014)**.
[2] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication", Proc. IEEE, vol. 8, no. 7, **(1999)**, pp. 1167-1180.
[3] S. B. Solario and A. K. Nandi, "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling," In Proc. EUSIPCO09, **(2009)**, pp. 824–832.
[4] S. Mallat, "A wavelet tour of signal processing: the sparse way," **(2009)**, 3rd ed. Academic Press.
[5] H. Farid, "Image forgery detection. IEEE Signal Processing Magazine," vol. 26, no. 2, **(2009)**, pp. 16–25.
[6] J. Fridrich, D. Soukal and J. Lukas, 'Detection of Copy-Move Forgery in Digital Images," In Proceedings of Digital Forensic Research Workshop, **(2009)**, pp. 1-10.
[7] P. Deshpande and P. Kanikar, "Pixel Based Digital Image Forgery Detection Techniques," International Journal of Engineering Research and Applications (IJERA), vol. 2, no. 3, **(2012)**, pp. 539-543.
[8] 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), **(2013)**.
[9] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions," Technical Report,TR 2004-515, Department of Computer Science ,Dartmouth College, **(2004)**.
[10] J. Hu, H. Zhang, Q. Gao and H. Huang, "An Improved Lexicographical Sort Algorithm of Copy-Move Forgery Detection," In 2nd IEEE International Conference on Networking and Distributed Computing, China, **(2011)**, pp. 23-27.
[11] S. Mukherjee, S. Kumar and J. Desai, "A Fast DCT based Method for Copy-Move Forgery Detection," In Proceedings of IEEE 2nd International Conference on Image Information Processing, **(2013)**, pp. 649-654.
[12] G. Li, Q. Wu, D. Tu and S. 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 China, **(2007)**, pp. 1750-1753.
[13] J. Zhang, Z. Feng and Y. Su, "A New Approach for Detecting Copy-Move forgery in digital images," In IEEE International Conference on Communication systems China, **(2008)**, pp. 362-366.

[14] 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.
[15] M. Zimba and S. Xingming, "DWT-PCA (EVD) based copy-move image forgery detection," In International Journal of Digital Content Technology and its Applications, vol. 5, no. 1, **(2011)**, pp. 251-7.
[16] M. Zimba and S. Xingming, "Fast and Robust Image Cloning Detection using Block characteristics of DWT coefficients," In International Journal of Digital Content Technology and its Applications, vol. 5, no. 7, **(2011)**, pp. 359-366.
[17] S. A. Fattah, M. Ullah, I. Ahmmed and C. Shahnaz, "A Scheme for Copy-Move Forgery Detection in Digital Images Based on 2D-DWT," IEEE Transaction, **(2014)**, pp. 801-804.

Authors

Anuja Dixit, she is a Research scholar pursuing M.Tech from Madhav Institute of Technology & Science, Gwalior, India. She has received B.Tech degree in Computer Science and Engineering from University Institute of Engineering and Technology, CSJM University, Kanpur, India.

Rahul Dixit, He is a research scholar pursuing Ph.D. from National Institute of technology, Rourkela, India. He has received M.tech. degree from IIT Dhanbad, India. His area of specialization is Multimedia security.

R. K. Gupta, He is a Head & Professor in CSE/IT Department at Madhav Institute of Technology & Science, Gwalior. He has received Ph.D. degree from Indian Institute of Information Technology and Management, Gwalior. He has received M. Tech Degree in Computer Science and Engineering from Indian Institute of Technology, Delhi, India. His area of specialization is Data Mining. He has guided several Master's and Ph.D. thesis.