IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, August 2015.
www.ijiset.com
ISSN 2348 – 7968

Noise variance estimation to detect forgery in digital images

Savita Walia[1], Mandeep Kaur[2]

[1] IT, UIET, PU
Chandigarh, India

[2] IT, UIET, PU
Chandigarh, India

Abstract

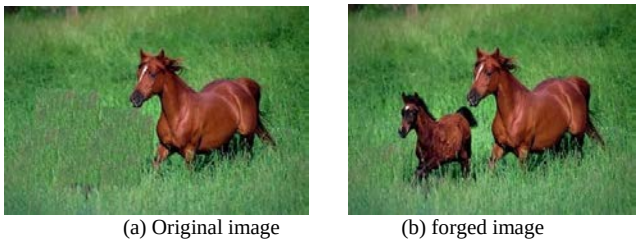
To maintain integrity and authenticity of the images, forgery detection techniques are used. But, the forgery creators try their best to hide the traces of the tampering in the image. Noise is the most commonly used means for this purpose. In an authentic image, the noise variation is supposed to be consistent throughout the image. In this paper, an existing method of detecting forgery using noise inconsistencies is analysed on a CASIA Tampered Image Detection Evaluation databases in order to check the accuracy of the method. It is based on the noise variance estimation with the use of PCA. For clustering of noise variance estimation of each block of the segmented image, an unsupervised clustering algorithm is used to divide blocks into groups depending on the estimated noise variance values. For further refining of the clustered results of blocks of each image, a supervised clustering algorithm is used.

Keywords:: *Image forgery, noise estimation, authenticity, image forensics, blind verification*

1. Introduction

Digital images have become the most important part in our lives. Digital photo images can be seen everywhere now-a-days, on the magazine covers, in newspapers and all over the internet. They are being widely used in military, education, forensics, communications, aerospace engineering, industrial purpose, scientific purpose, etc. The viewers of these images need to be aware that seeing does not always imply believing. With the increasing use of the internet, the photo editing have become easy, even a novice can also edit an image with the help of basic tools that are freely available on the internet. There are many freeware tools available which are used by professionals to alter the images. To maintain the integrity and authenticity of the images, forgery detection methods are required. Image can be forged in various ways; some of the most common types of forgeries are copy-move, splicing, lightening adjustment, geometrical transformations, etc. One such example is shown in figure 1. The copy-move is created by copying a region from one image and then pasting into another to add/ hide some object in the image. It is also called as cloning.

To verify the originality of the images, forgery detection methods [1] are required which help in security and copyright protection of images. The methods available for forgery detection are divided into two categories: active and passive methods of detection. Active methods [2-3] require pre processing on the image which embeds a digital watermark or digital signatures which are carried out during the time of image generation. These methods are only useful when we have some information about the image like digital signature or watermark so as to compare it with the ones in the image under consideration. For blind verification of the images, the passive methods are used these days. They do not require the embedding of digital watermark or digital signatures into the image during creation.



(a) Original image (b) forged image

Fig.1 Example of forgery

Various passive methods [4-6] are available for each kind of forgery. For example, to detect geometrical transformations, resampling technique is use. To detect spliced images, boundary based techniques are used most of the existing methods are based on certain type of input images i.e. for spliced images, a different approach is used. The same approach cannot be used to detect another kind of forgery. To overcome this problem, a falseproof method is required which is independent of the input image or which can detect any kind of forgery based on certain intrinsic features of the image. One of such feature is noise.

Noise has a negative impact on the perceived quality of the image. The additional noise is included in the image

ISSN 2348 – 7968

with the purpose of hiding some marks of the tampering. Most of the methods fail in the presence of excessive noise. There exist a method in which noise variance is estimated with the help of principal component analysis and the blocks are classified on the basis of that noise variance.

The paper is based on the estimation of noise variation to detect forgery [16]. The noise variance of each block is estimated using principal component analysis. In PCA, the covariance matrix of each block is calculated and the smallest eigen value of that block is the estimated noise variance.

The paper is organised as follows. Section II presents a brief discussion on previous work related to this field. The experimental work is discussed in detail with the methodology in section III. Results and discussions are provided in section IV. The paper is wrapped up in the conclusion at the end of the paper in section V.

2. Previous Work

The noise features of the image are being widely used for forgery detection and steganalysis. A forensic analysis on images was performed by H.Gou and A. Swaminathan [7] in which three sets of features based on noise properties of the image are extracted. Firstly, the features are extracted from denoising operations, second set of features are extracted by doing a wavelet analysis and third set of features are obtained by prediction of neighbourhood. It is observed that the manipulations in the image affect the non-gaussian properties of the image, that is why the wavelet coefficients are extracted. Once all the three features are extracted, a robust classifier is built for distinction between the camera output and the manipulated image.

A.E. Dirik and N. Memon [8] proposed a detection method which was applicable to various operations like splicing, retouching, recompression, resizing, blurring etc. But it did not target any specific operation. The techniques which focus on such tampering are named as ‘Targeted Tamper Detection’. There are other class of techniques which focuses on tampering like filtering, splicing (up/down), rotation, compression etc. These techniques are called as ‘Universal Tamper Detection’. Third types of methods include Localized tamper detection which includes tampering like sensor noise pattern, Color filter array demosaicing artifacts, chromatic aberration, etc. In this paper, the technique for local and global tamper detection has been proposed by the authors. The major difference in other global techniques and this technique is that this uses a threshold value for detecting the artifacts whereas other global methods use a complex classifier to make a decision about the artifacts. The database was collected from 10 different camera models. The major drawback of this method is that it is sensitive to JPEG compression/re-compression and resizing. It may also fail for smaller artifacts.

Another very effective and reliable method of estimating noise standard deviation of an image is proposed by S. Pyatykh, J. Hesser and L. Zheng[9]. In this method, the noise variance estimation is calculated using principal component analysis of image blocks. The PCA approach does not assume the presence of homogeneous areas in the image under consideration. PCA has the ability to process any type of images including textures and the ones which have high frequencies. There are some other approaches like Discrete Cosine Transform of an image. DCT approach uses self-similarity to separate the signal from the noise in the image. The paper presents the comparison of PCA approach with various other methods. This paper presents a technique which evaluates the least eigen values of the covariance matrix of the image blocks. The PCA approach can also be used in image segmentation and compression applications which require the estimation of the noise level variance. In denoising applications, a careful choice of the noise estimator is utterly important.

The authors M. Chen, J. Fridrich, M. Goljan and J. Lukáš[10] used the censor noise to estimate the image’s. In this paper, an integrated method for recognition of source camera from the images taken for detecting images that are digitally forged with the help of photo response non-uniformity noise(PRNU) which is a distinctive stochastic characteristic of imaging sensor. A maximum likelihood estimator is calculated using simplified representation of the sensor output. The regions of the image are operated for detection of forged regions by distinguishing sensor PRNU. The camera recognition and image integrity is obtained with the help of detection of PRNU of each pixel in the image. The maximum likelihood principle is used to estimate the PRNU. The identical model is then used to put together the job of identifying PRNU as the hypothesis testing problem with the use of Neyman-Pearson criterion.

Image noise is the dissimilarity of brightness of pixels fundamental in the image pre-processing. X.Pan and X. Zhang[13] proposed a method in which the forgery is detected using noise variances. Clustering of blocks is used to group the blocks. Noise variances are calculated using natural properties of the image using Discrete cosine transform The main advantages of this method are that it donot require any knowledge of the image beforehand and kurtosis of the image need not to be estimated. The spliced images can also be detected by this method.the main drawback of this method is that it cannot detect images having lower noise variances; the method detects higher variance images easily.

ISSN 2348 – 7968

J. Fan et al [14] proposed a detection method based on EXIF parameters of the image to associate statistical features of the image noise. The EXIF features are closely related to camera click settings. Further, least square weights are used for regression analysis of the features. This method works well for contrast enhancements as well as brightness adjustments, as brightness and contrast are the basic targets while forgery is done.
Babak Mahidian[15] formulated a method in which forgery is detected with the help of noise inconsistencies in the image. The major drawback of this method was that it can not detect forgery in which there are no homogeneous areas.Another drawback is that it cannot detect defects where noise degradation is quite small. It overcomes the drawbacks of previous method in which kurtosis was estimated due to which numerical errors appear. Noise estimation is done using tiling of the image using high pass filter and then doing a wavelet analysis on the image. Then, on the basis of homogeneity of the areas in the image, classification is done.
Another major research in this area is proposed in [16]. In this method, the noise estimation is calculated using principal component analysis of the image which is based on the eigen values of the image. For further classification, a hybrid technique is used which uses k means for unsupervised clustering and then SVM for refining of the data. This method was not tested on standard databases

3. Experimental Work

In this paper, a method based on noise estimation is used to detect and locate the forgeries done to the image which is discussed in this section.

3.1 Image Pre-processing

Firstly, the color space of the image is changed. If the image under consideration is in RGB colorspace then it is transformed into HSV colorspace where HSV is Hue Saturation Value. It is also called as HSB i.e. Hue Saturation Brightness. HSV is basically the transformation of RGB colorspace. It is a belief that HSV colorspace is more natural than other colorspaces. Color is more naturally expressed in terms of Hue and saturation than in terms of addition and subtraction of color components. HSV colorspace is preferred over RGB due to the reason that HSV separates the luma or the image intensity from the chroma or the color information. This is very useful as we only want to extract the saturationcomponent of the image. Rest all procedure has been implemented on saturation component. So the saturation component has been extracted from the HSV colorspace after transformation from RGB colorspace. Next step is to segment the image into blocks. The block size plays a significant role in the accuracy and efficiency of the system. The larger the block size, the chances of detecting smaller forgeries decreases. It has been proved in previous work that the block size of 32*32 gives more reliable and accurate results as compared to other block sizes like 8*8, 16*16/, 64*64, etc.

3.2 Estimation of Noise variance

Once the image is segmented into blocks, the noise features of each block are extracted. The noise variance estimation is performed using Principal component analysis on each segmented block. PCA is highly computational and has the ability to work on images with textures, even if there exist no homogenous regions.

3.3 Clustering: Detection of forgery

Unsupervised clustering is performed to divide this dataset into clusters (Fig. 2). Clusters are formed on the basis of the variation in the dataset. K-means algorithm is used to implement this which gives the rough analysis of the blocks. It divides the blocks into two clusters. If the image under consideration is authentic then the clusters will not be formed. In original images, either one or both of the centroid values are in imaginary numbers. If centroid values are real, then the image is considered as forged.

3.4 Classification and locating forged blocks

To refine the clustering results, a supervised technique is used (Fig. 3). In our method LSSVM classifier is used for classification. LS-SVM stands for Least Squares Support Vector Machine and is a version of Support Vector Machines. LS-SVM is a set of supervised learning methods which are used for classification and regression study by analyzing the data and recognizing the patterns. LSSVM comes under the class of kernel based learning techniques.
The kernel function used in LSSVM is RBF kernel i.e. the (Gaussian) radial basis function kernel. It is the most widely used kernel function in most of the kernel base algorithms in SVM classification. The procedure of clustering and classification is given in figure 2 and 3. To refine the output of k-means, the one-third of the blocks near the centroids is considered for training purpose.
Further classification is done on the basis of training dataset. The cluster which is left with minimum number of blocks is assumed to be forged and the rest of the blocks are authentic.

ISSN 2348 – 7968

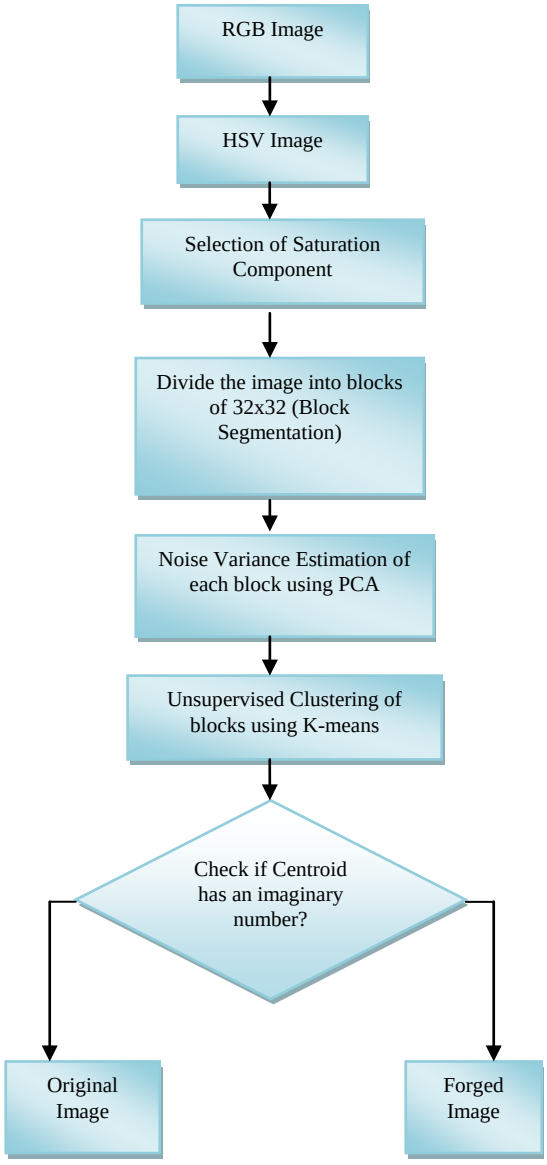


Fig.2 Forgery Detection

4. Results and Discussion

The existing method has been experimented on the images taken from CASIA Tampered Image Detection Evaluation dataets, i.e. CASIA version 1.0 and CASIA version 2.0. The database contains both the forged and authentic images. The image under consideration goes through the addition of Gaussian noise of varying mean and standard deviation. Block segmentation is carried out which segments the image into 32*32 size blocks. Then the noise variance is estimated. An unsupervised clustering technique (k-means) is used to cluster the data on the basis of the estimated noise variance values. The results of unsupervised clustering are shown in Fig. 4. If the k-means gives clusters with centroids having values in imaginary numbers then the image under consideration is authentic otherwise it is forged.

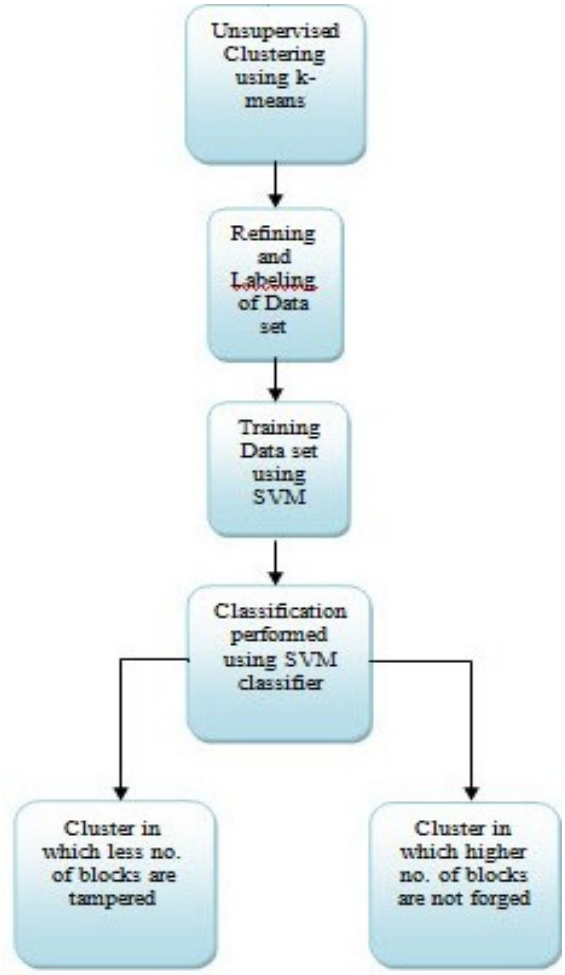


Fig.3 Locating forged blocks

LS-SVM classifier is used to classify the clustered results. The output of the SVM classifier is shown in Fig 5. The forged blocks are located on the image using the formula given in Eq(1):

```
((i-1)*32,(j-1)*32,32,32)          Eq(1)
```

where i and j are the indices.

ISSN 2348 – 7968

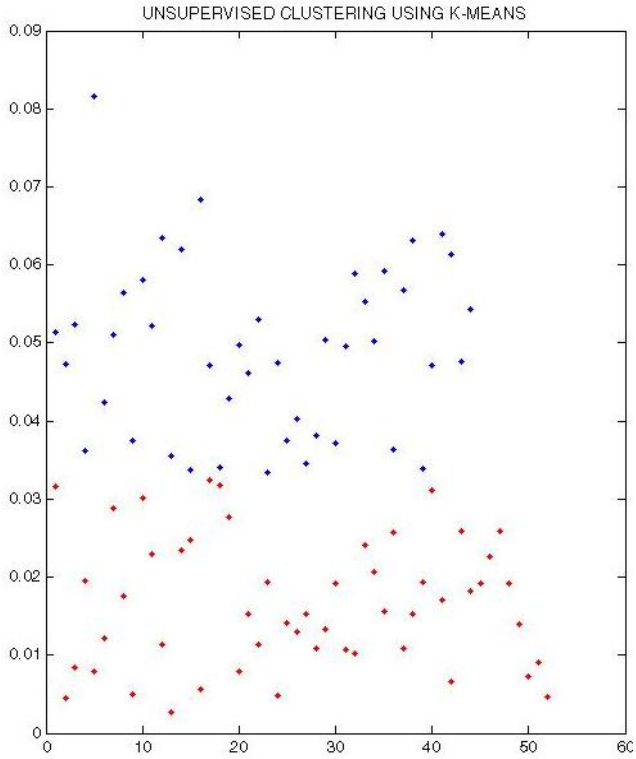


Figure 4. Unsupervised Clustering (K-means)

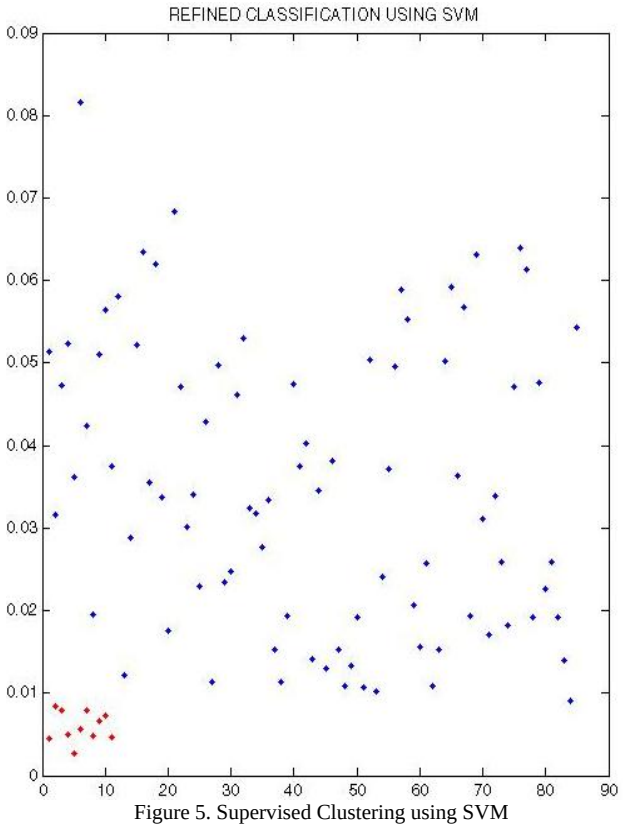


Figure 5. Supervised Clustering using SVM

The observations that are obtained while using this method on standard databases are given in Table 1 and table 2. The image sizes in CASIA are 256*384 and 384*256. CASIA 1 contains JPEG image formats where as CASIA 2 contains authentic images in JPEG format and tampered images in JPEG and TIF file formats.

Table 1

CASIA 1						
No. of Images (1721)		TP	TN	FP	FN	Accuracy %
Au	Sp					
800	921	559	567	241	254	65.43

Table 2

CASIA 2						
No. of Images (2000)		TP	TN	FP	FN	Accuracy %
Au	Sp					
1000	1000	621	707	379	293	66.4

The detected forgery in an image is shown below in Fig. 6

Fig. 6 Detected forged blocks in the image

5. Conclusion

A reliable method of detecting and locating the forgeries in an image is used in this paper. The method is tested on the standard database (The Institute of Automation, Chinese Academy of Sciences, CASIA).The results show that the method effectively detects the forged blocks and classifies them and gives the accuracy of 65.43% and 66.4% on CASIA1 and CASIA2 respectively. The forged blocks can be effectively shown on the image as well. Further, the accuracy of the method can be improved by combining the existing method with some other features.

ISSN 2348 – 7968

References

[1] H.Farid, ”Image Forgery Detection”, IEEE signal processing magazine, March 2009, pp. 16-25.
[2] R.G. Schyndel, A. Tirkel, and C.F Osborne, “A Digital Watermark”, Proceedings of IEEE International conference on Image Processing, ICIP, 1994, pp. 86-90.
[3]J. Fridrich, "Image Watermarking for Tamper Detection," Proceedings of the IEEE ICIP, Oct 1998, vol. 2, pp. 404-408.
[4] B. Mahdian,, S. Saic, “Blind methods for detecting image fakery”, IEEE Aerosp. Electron. Syst. Mag., 2010, Vol. 25, Issue 4, pp. 18–24.
[5] R.E.J. Ranty, T.S. Aditya, S.S. Madhu, “Survey on passive methods of image tampering detection”. International Conference on Communication and Computational Intelligence (INCOCCI), 2010, pp. 431–436.
[6] W. Luo, Z. Qu, P. Feng, J. Huang, “A survey of passive technology for digital image forensics”, Front. Computational Sciences China, 2007, Vol.1, Issue 2, pp. 166–179.
[7] H. Gou, A. Swaminathan, M. Wu, “Noise Features for Image Tampering Detection and Steganalysis”, Proceedings of the IEEE International Conference on Image Processing, 2007, pp. 2893-2896.
[8] D. A. Emir, N. Memon, “Image Tamper Detection Based on Demosaicing Artifacts”, Proceedings of the 16th IEEE International Conference on Image Processing (ICIP), 2009, pp. 1497-1500
[9] S. Pyatykh, J. Hesser and L. Zheng, “Image Noise Level Estimation by Principal Component Analysis”, IEEE Transactions on Image Processing, 2013, Vol. 22, Issue 2, pp. 687-699.
[10] M. Chen, J. Fridrich, M. Goljan and J. Lukáš, “Determining Image Origin and Integrity Using Sensor Noise”, IEEE Transactions on Information Forensics and Security, 2008, Vol. 3, Issue 1, pp. 74-90.
[11] A. C. Popescu, “Statistical Tools for Digital Image Forensics”, Proceedings of the 6th International Workshop on Information Hiding & LNCS, 2004, pp. 128-147.
[12] S. Walia, M. Kaur, “Forgery Detection using Noise Inconsistency: A Review”, International Journal of Computer Science and Information Technologies, 2014, Vol. 5, Issue 6, pp. 7618-7622.
[13] X. Pan, X. Zhang, S. Lyu, “Exposing Image Forgery with Blind Noise Estimation”, Proceedings of the Thirteenth ACM Multimedia Workshop on Multimedia and Security, 2011, pp. 15-20.
[14] J. Fan, H. Cao, A. C. Kot, “Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection”, IEEE Transactions on Information Forensics and Security, 2013, Vol. 8, Issue 4, pp. 608 – 618.
[15] B. Mahdian, S. Saic, “Using Noise Inconsistencies for Blind Image Forensics”, Image and Vision Computing, 2009, Vol. 27, Issue 10, pp. 1497-1503.
[16]Y. Ke1, Q. Zhang, W. Min, S. Zhang, “ Detecting Image Forgery Based on Noise Estimation”, International Journal of Multimedia and Ubiquitous Engineering, 2014, Vol.9, Issue 1, pp.325-336.
[17] [14]J. Lukáš, J. Fridrich and M. Goljan, “Digital Camera Identification from Sensor Pattern Noise”, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, (2006), pp. 205-214.
[18] Y. Sutcu, S. Bayram, H. T. Sencar and N. Memon, “Improvements on Sensor Noise Based Source Camera Identification”, Proceedings of the 2007 IEEE International Conference on Multimedia and Expo, (2007), pp. 24-27.
[19] D. Zoran and Y. Weiss, “Scale Invariance and Noise in Natural Images”, Proceedings of the IEEE 12th International Conference on Computer Vision, (2009), pp. 2209-2216.
[20] http://forensics.idealtest.org:8080/
[21] http://forensics.idealtest.org:8080/index_v2.html

Savita Walia received her B.Tech degree in Computer Science and Engineering from CTIT, Punjab Technical University, Punjab (India) in 2012 and persuing her Master’s in Engineering (Information Technology) from Panjab University, Chandigarh (India).Her area of research is Digital image processing and Image forensics.

Mandeep Kaur received her B.Tech degree in Computer Science and Engineering from BCET, Punjab Technical University, Punjab (India) in 1999 and received her Master’s in Engineering (Information Technology) from PEC, Panjab University, Chandigarh (India) in 2004. She is associated with University Institute of Engineering and Technology, Panjab University, Chandigarh (India) since 2005. Her area of interests includes Digital image processing and Image forensics.