International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 125-140
http://dx.doi.org/10.14257/ijsia.2015.9.4.13

Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier

Mohammad Farukh Hashmi[1] and Avinash G. Keskar[2]

[1-2]Department of Electronics and Communication Engineering
[1-2]Visvesvaraya National Institute of Technology, Nagpur, 440010, India
farooq78699@gmail.com, agkeskar@ece.vnit.ac.in

Abstract

Image forgery is a major issue in today's digital publishing and printing. Now a day's system can be used for forensic purpose to validate the authenticity of an image. In this paper we present an approach for image forgery authentication. We observe that a non morphed and non forged image shows homogeneity in non spectral domain. This homogeneity is lost when any forgery or morphing is applied on the images. We therefore apply a set of transform over the images. We combine DCT statistics, LBP features with curvelet statistics and Gabor transform of the images to represent an image in the transformed domain. CASIA image dataset with seven thousand authentic and same numbers of tempered images is used to verify the technique. We divide the dataset into equal halves to perform training and testing. Transformed images are used to train Hidden Markov model as HMM can extract probabilistic state information from a large statistical model. A test images is tested in transformed domain by HMM with log likelihood estimator. In case HMM returns an indeterminist result or multiple subset of result, the transformed test image is tested with two class SVM classifier with RBF kernel. Results show that the accuracy of the system is over 89% for 500 test instances.

Keywords: *Image forgery; Local binary pattern (LBP); Gabor filter, Curvlet transform, Discrete Cosine Transform (DCT); Support Vector Machine (SVM); Hidden Markov Model (HMM).*

1. Introduction

Image forgery is a major issue in today's digital publishing and printing. Accepting the authenticity of the images is quite difficult as most of the digitally published images are forged before publishing. For instance in political rallies often numbers of listeners are digitally changed to show many attendees. Therefore image forensic with forger detection has become a major challenge. Image presented as digital evidence might be forged and therefore is tough for being considered as valid. There are some previous works in the direction which depends upon detecting copy paste forgery only. Image forgery is the approach of modification the imaging information from the images using image-processing software packages like Photoshop, other image editor tools. It is also Methods for manipulating the original information by using various transformation techniques such as resizing, blurring, scaling and rotation, addition of noise, adding and removing any object and applying various other types of manipulation for hiding the real data inside the picture To provide a digital photo as evidence proof for any criminal case, there is a requirement of the identification of the genuineness of the photo. Image Tampering can be divided into as a copy move forgery and as a non copy move forgery. In a copy move forgery, some portion of the image is copied and added in any other place of the image so that there are no modifications like resizing, blurring etc.In the other case, because of the earlier explained modification techniques; the information becomes extremely similar

ISSN: 1738-9976 IJSIA

[1].We apply forgery detection approach to recognize the tampered portion of the image on the basis of correlated information. Due to development of digital imaging technologies, it has become terribly simple to preserve any event of a digital image and this digital imaging data is being widely utilized for various multiple applications like including surveillance system, multimedia, forensic applications, electronic media and scientific discoveries. However, recent progress of sophisticated editing software programs, any person can easily tamper and damage the available information of the image. Such motivation is require for understanding the use of techniques that can be used for identification and validation of authenticity of digital information [1].

2. Related Work

There are several image forgery detection techniques already proposed by different authors [29]. Most of these techniques are devised for detecting one specific type of image forgery. For example techniques that can detect image forgery where objects are morphed in the image from the same image cannot detect the forgery where object morphing source is different from current image source [2].A lot of work has been previously done in forgery detection, particularly copy-move forgery detection. Popescu et al. [3] devised a method for forgery detection by dividing the image into several blocks, applying the PCA transform (for dimension reduction) and detecting the forgery by detecting similarity between the blocks. Zach et al. [4] devised a method of forgery detection through classification of JPEG ghost.Hao-Chiang Hsu et al. proposed copy-move forgery detection by detecting the similarity using feature extraction by Gabor filter [5]. Leida Li et al. [6] devised a method for copy-move forgery detection using Local Binary Patterns. M.Qiao et al. [7] used curvelet statistics for detection of copy-move forgery after dividing the image into several overlapping blocks. B.L.Shivakumar devised a method for detection of copy-move forgery using Harris Interest Points and SIFT descriptor [1]. S. Khan and A. Kulkarni devised a method for copy- move forgery detection using the multi-resolution characteristic of DWT [8]. In their work, DWT was used for reducing the dimensions of the image and then analyzing it. Fridrich et al. analyzed the DCT coefficients of image blocks, performed lexicographical sorting and outputted the copied regions by detecting similarity between the blocks [9]. Irene Amerini et al. proposed a SIFT based method for copy-move attack detection [10]. Local visual features like SURF, SIFT, GLOH are robust to several geometrical transformations like rotation, occlusions, clutter and scaling. Hence they are being extensively used for image forgery detection. Use of machine learning techniques for image forgery detection is relatively new. E.S.Gopi et al. used Auto Regressive coefficients as feature vectors and ANN for training the system [11].HMM and SVM were used majorly for speech recognition, signature verification, license plate detection and classification etc. E.Justino et al. used SVM and HMM classifiers for off-line signature verification [12]. S.Impedovo suggested a bank cheque processing system using HMM based algorithms [13]. P.Sutthiwan et al. used multi-size block based DCT transformation along with SVM classification for detection of image forgery [14]. Jia Li et al. studied image classification using 2-D HMM [15].

Image forgery detection is a tough challenge due to various resolutions and standards of image capture devices. Work in this direction leads to analysis of the images in the transformed domain. DCT, Gabor, Curvlet and other transforms techniques have been most significant domain of analysis of images for forgery. However most of the techniques fail to produce neutral result. i.e. irrespective of training and testing database. Further different techniques are developed to mark different category of image forgery. The objective of this work therefore is to develop a comprehensive technique to detect any type of image forgery with the help of machine learning technique. It is shown that prior knowledge and machine learning significantly improves the belief coefficients of the algorithms about forgery and natural images. The objective is also to analyze the performance of the technique with CASIA forgery dataset which includes natural images, architectural images and animal & texture images such that the technique can be claimed to be neutrally performing detection over any category of images [16]

3. Problem Statement

Now a day's system can be used for forensic purpose to validate the authenticity of an image. The technique can also be used by digital publishers to authenticate the naturalism of an image before purchasing the copyright. The images can be tested by digital image libraries to check the authenticity of photographs being offered by photographers. With images incorporated in the web security like personal banking, this technique can be used to check the phishing attack by finding the forged images. The statement of the work can be simplified as detection of forgery in images by combining HMM and SVM classifier and using combined features of DCT, Curvelet, LBP and Gabor Transform. Image forgery detection can be used by several photographic conventions and contests where prizes are awarded based on beauty and uniqueness of the images. The proposed technique is dependent on machine learning. Therefore large amount of training data is needed for the images to be classified accurately. As the machine learning depends upon detecting image features in the transformed domain, images must be of large size in order to retain the features after transform. As the images can be under different lights, the transforms must take care of rotation and light variations. Curvelet and Gabor transform are both block transform where transform is applied on the subset of images, either in the polar component or in the spectral blocks. Therefore feature extraction process is time consuming. Most importantly HMM considers each image as an independent class. Therefore numbers of iterations increase significantly with the increase in number of instances. A Baum-Welch algorithm has been tested for training and classification of forgery application. The probability of a forged images detection and classification by a HMM is calculated, and the decision of the authenticity of available images from the database is made available on the basis of threshold [17].

4. Methods and Materials

In this section, we shall have a look at the elementary paradigm and concordant aspects regarding Image Authentication. The paradigm assumes a holistic approach and gets bifurcated into Feature Extraction Algorithms and the Classification (Machine Learning) algorithms. The primitive Feature Extraction techniques include feature convergence by transforms and methodologies like Gabor Filter, Curvelet Transform, Discrete Cosine Transform (DCT), and Local Binary Pattern (LBP). On the other hand, for the effective classification of Image Forgeries (Authentication), we have used Machine Learning Algorithms like the Hidden Markov Model (HMM) and the Support Vector Machine (SVM). Basic building blocks of image forgery and classification System is illustrated in Figure 1. [16]

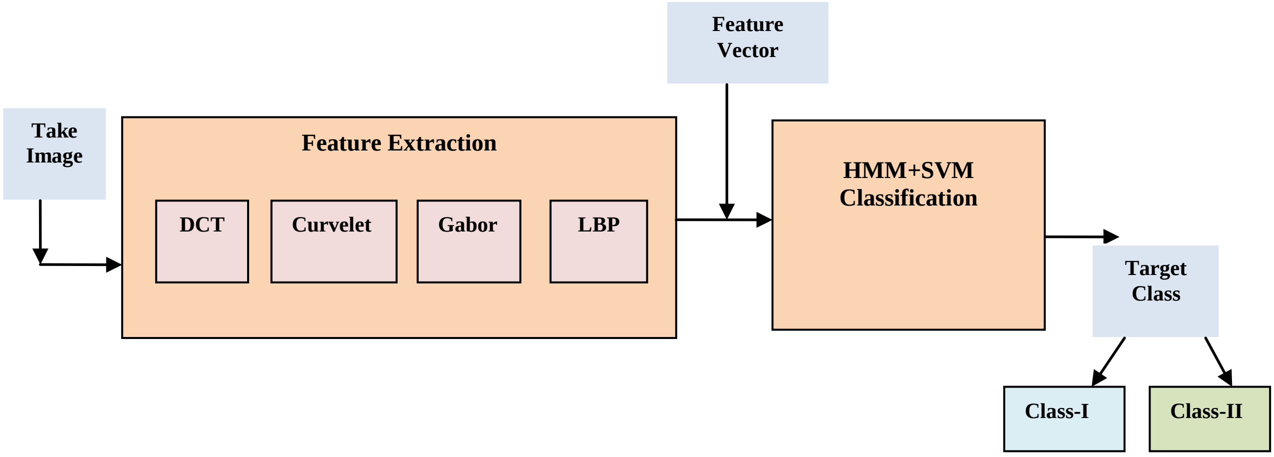

Figure 1. Basic Building Blocks of Image Forgery and Classification System

4.1. Algorithm for Extraction of Image Features

1. **Calculate Features using DCT Transform**

```
Step 1: First we take an image
Step 2: Convert to image in gray scale form
Step 3: Apply DCT transform on the image
Step 4: Apply next magnitude component
Step 5: Calculate features as Mean, Standard Deviation form.
```

2. **Calculate Features using LBP**

```
Step 1: First we take image
Step 2: Convert to given image into Gray Scale
Step 3: Declare a window for next processing
Step 4: Place the window around each pixel
Step 5:  Next, check if the pixel in window>center
                Value=1
        Else
                Value =0
Step 6: Generate binary pattern with values 1, 0
Step 7: Convert binary to decimal and replace in center pixel
Step 8: Normalize the Image
Step 9: Calculate Mean, Standard Deviation for feature calculations
```

3. **Calculate Features using Gabor Filter**

```
Step 1: We will take a test image
Step 2: Convert the image in gray form
Step 3: Declare Gabor kernel for the given image
Step 4: Next we will take a window
Step 4: Multiply pixels in window with Gabor kernel
Step 5: Replace the this value to center pixel
Step 6: Normalize the values
Step 7: Calculate Features: column wise mean (if image size is 256x256)
Obtained total features=256
```

4. **Calculate Features Using Curvlet**

Step 1: First we will take test image from the data base
Step 2: Apply gray scale conversion
Step 3: Next we will calculate FFT transform of the given image
Step 4: Next rotate the processed transform image for further processing
Step 5: Calculate Curvlet of the processed image
Step 6: We will calculate features: Mean and standard deviation of 16 Curvelet matrices obtained through 16 rotations

4.2. Algorithm for Classification using HMM and HMM+SVM

The proposed image forgery detection and classification verifies the authenticity of the images available in CASIA data bases. The design procedure is divided into following stages:-

a) Training procedure

All Images from the database available in CASIA are modeled by estimating the parameters of the images for HMM for available set of observations. A set of images from the each authentic and tampered image database are used to train each data set of HMM. Features extracted from each block of the images are used to calculate the observation vector parameters. These Parameters are chosen on the basis of maximum likelihood condition that maximizes the likelihood criterion of the observation data (O) of the images. This maximization process is computed using the Baum-Welch algorithm [18]-[19]. The following steps are followed and applied [20].

Firstly, the value for HMM λ = (a, b, j) is initialized. All training images from the database are divided into 4 states (s1, s2, s3 and s4) and observation vectors obtained from the trained forged and authenticate images are clustered into m dimensional vector using k-means algorithm [19]. The values computed are used to find the initial estimation of the observation probability matrix b. The initial values for a and j are set from the left to right position of the HMM topology [20].

The next process is to re-estimate obtained model parameters using equation Baum-Welch algorithm in order to maximize the P (O /λ). The iteration stops when the difference between the likelihood values of the current iteration (k+1) and those of the previous one (k) iteration is smaller than a preset threshold (H) as available in below equation (1).

b) Recognition and Classification Results

In the recognition stage, a set of 500 genuine and forged images are used to determine the recognition ability of the proposed system. As it was done in the training stage, the extracted feature vectors from each of the states of the test images are used to form the observation vectors. The trained HMMs are used to compute the likelihood function as follows:

(1) Given O (t) as the DCT, Gabor, Curvelet, LBP and various other Transform techniques based observation sequence generated from CASIA images database is to be recognized.

(2) The probability of the observed vector given each image model P (O (t)/λi) is computed using Viterbi algorithm [18]-[19].

(3) The observed vector is labeled with class model which maximize the probability P (O(t)/λi).

(4) A test image (t) from the authentic and forged images database is recognized as authenticity of the image (k) in the database if: P (O (t) /λk) = maxn P (O(t) /λi) [20].

129

c) Classification using HMM+SVM

The test image features are compared with trained image features using the log likelihood estimator. When the HMM process detects a class, the iteration is stopped. However when the likelihood value is infinite with respect to all training instances, the image is tested with SVM. As SVM is a two class classifier, the detection is accurate and fast. We have proposed the SVM+HMM approach.

Support Vector Machines (SVMs) are machine learning algorithms that use a high dimensional feature space and estimate differences between classes of given data to generalize unseen data [21]. The database of 500 images i.e. 250 authentic and 250 forged images are used for training thus a total of 500 Images for training and testing the system.

5. Proposed Algorithm

In this paper a methodology has been proposed for detecting whether a given image is forged or not using HMM and SVM classifiers. The image is represented by its model in the transformed domain in terms of its feature vector. Feature extraction is accomplished by DCT, LBP, Gabor filter and Curvelet transform. A detail on the methods of feature extraction is given in the sections to follow. The feature vectors are normalized by dividing them by the maximum of their values and multiplying them by 50. Since HMM can process only non-zero values, 1 is added to all feature vector values. A feature vector set is thus generated for each image. The system is then trained. Training is performed using 250 authentic and 250 forged images. The images are randomly selected from the CASIA image database of authentic and forged colored images released by the Institute of Automation, Chinese Academy of Sciences. The trained HMM and SVM models are then used to detect image forgery. During testing, a comprehensive feature vector set of the test image is generated. Firstly, data classification is done by HMM. A search is performed for the best combination of states for the maximum a posteriori possibility. This is performed by what we call the 'log likelihood' estimator, details of which are provided in the appropriate section. When the likelihood value is infinite, we have to classify the image by SVM. Recall the system is already trained by SVM. The image is then classified in to either Class I (Authentic image) or Class II (Forged image). The whole process is encapsulated in the flowcharts shown in Figure 2.We have prepared a comparative study between image classifications by just HMM & by using HMM and SVM. It was found that better image classification and thus forgery detection is possible when we use both HMM and SVM. The same has been demonstrated in the analysis of results of our work.

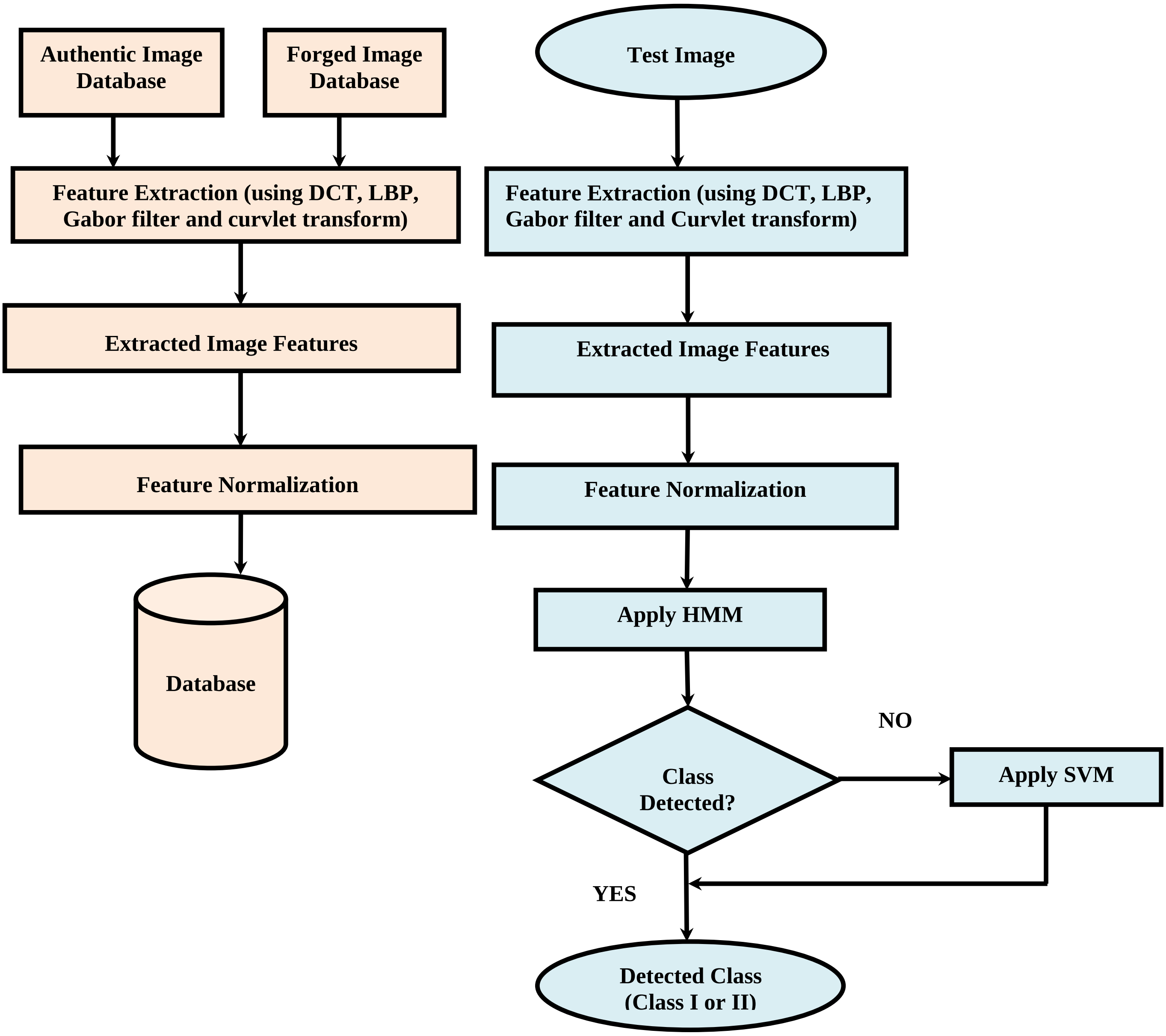

Figure 2. Flow Chart for Training Phase and Testing Phase

6. Implementation of Proposed System

The proposed forgery detection and classification algorithm consists of two stages as shown in figure 3 which are feature extraction with HMM and support vector machine (SVM) classification. The feature extraction process is composed Gabor wavelet transform, DCT, Curvelet and LBP, which extracts feature vectors for classification from CASIA images database. Figure 2 shows samples of authentic image and forged image and detected class for genuine and forged.

The proposed system depends upon extracting both local and global patterns from the images in the transformed domain to represent the underneath pattern of the image. We first perform an image resizing such that all the analyzed images are of same size. Images are first resized to 256x256.

We then apply 2D Gabor transform over the image. Gabor kernel produces non zero linear components that are essential for HMM. However Gabor filter is both phase and magnitude dependent. We therefore rotate the image from 0' to 360' in step of 10' and obtain features for each of these rotations to obtain rotation independent features.

DCT is performed on the images which gives frequency component of the image. Forgery in the image introduces high frequency component in the images. Therefore mean and standard deviation of the DCT values represent the forgery in a lucid way.

Any forgery invariably breaks the local texture information and introduces noise. Hence obtaining local texture description can be thought as a good enough measure of image forgery. We therefore perform LBP on the image with circular neighborhood with radius 5. This is done by first obtaining an nBin histogram from the image and then extracting local binary patterns [28].

Curvelet transform is a good measure of local image statistics in the polar domain. Unlike spectral domain, polar data can have limited orientation, from 0' to 360'. Wavelet can have infinite number of sub images. But curvelet is capable of generating finite set of images. Hence we extract 16 sub images from curvelet transform (as 16*16=256). We obtain mean and standard deviation of all these 16 images to form a comprehensive feature set [30].

We then combine all the mentioned features in a single matrix. As HMM expects finite states for analysis, we normalize the feature vector by dividing it with max of values and then multiplying the vector with 50. Hence all the features are now represented by values between 0-50. However HMM cannot process 0 values in the observation matrix. Hence we add 1 with the feature set such that no value is 0 in the feature vector.

Test image's features are extracted in the same way. These features are compared with the trained features using log likelihood estimator. When HMM detects a class, the iteration is stopped. If the likelihood value is Infinite with respect to all train instances, the system is tested with SVM. As SVM is a two class classifier, detection is accurate and fast. The reason of stacking SVM with HMM is that HMM can identify the hidden state from the features which is not possible with SVM. In case HMM produce infinity as the distance from training instances than that suggests that there are no hidden states [31]-[32]. Figure 4 and Figure 5 shows samples of authentic image and forged image and detected class for genuine and forged counterparts in the bottom row. Examples of authentic and forged images taken from the CASIA database [16] are shown in Below Figure 4 and Figure 5. Thus SVM can classify the linear data. Block diagram of proposed system using HMM and SVM classifier is shown in figure 3.

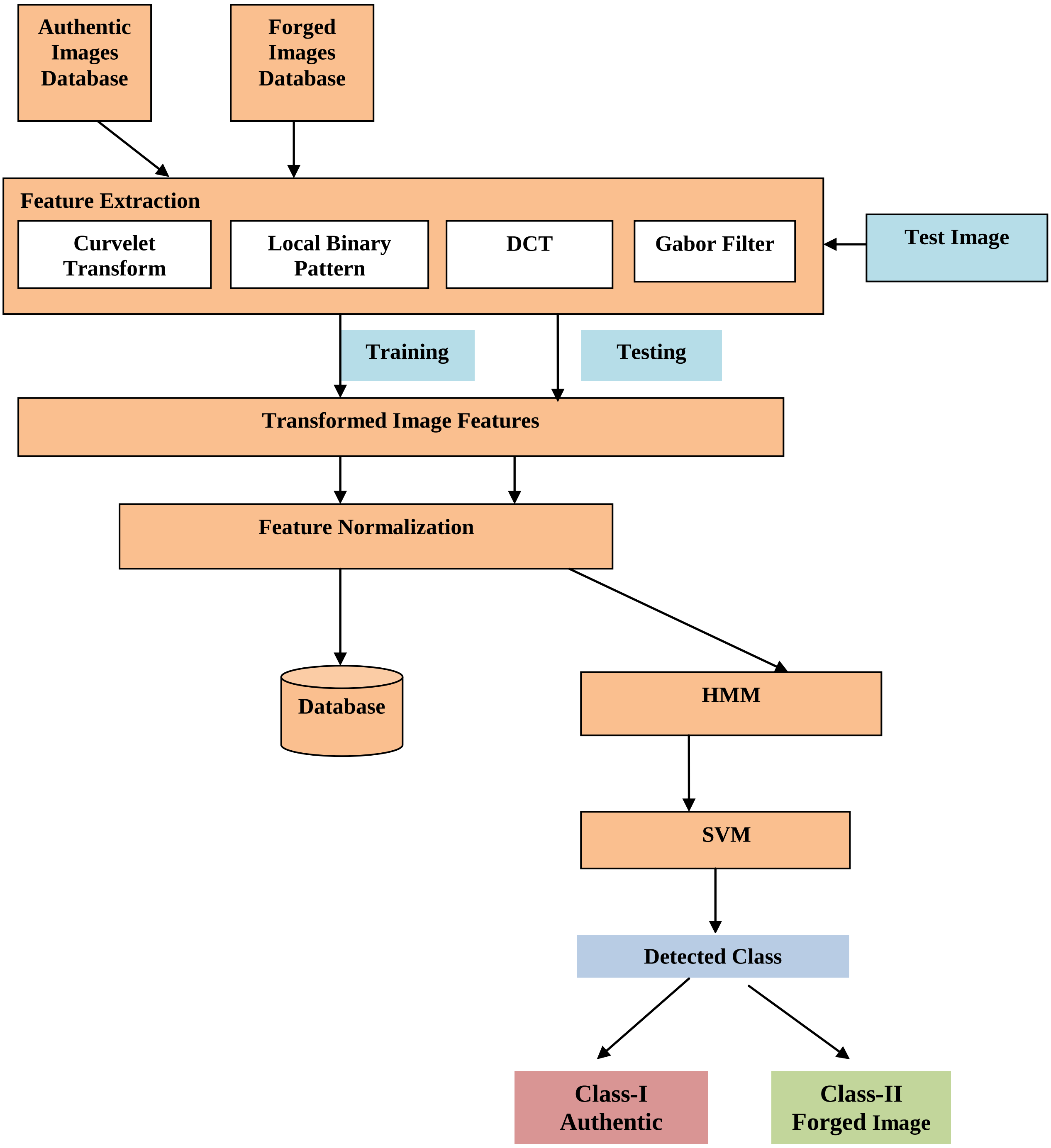

Figure 3. Flow Chart of Proposed System using HMM and SVM Classifier

133

Figure 4. Images Used For Testing and Detected Correctly As Authentic

Figure 5. Images Used For Testing and Correctly Detected As Tampered

7. Simulation Results and Discussion

As stated earlier, the images for training and testing were taken from the CASIA database. All the images were available in JPEG and TIFF format. 250 authentic images and 250 forged images were used for training the HMM and the SVM model. These 500 images were randomly selected. During testing, we divided the 500 images into 5 sets; each set consisting of 100 images. Each set was tested with the system tested with just HMM. After that each set was tested with system trained with SVM as well. Computation was performed in MATLAB and a library for support vector machines [21] was used. Since the images were selected randomly, the forgery in the image may be of any type described previously. Here we define a few terms:

TP (True Positive): Forged image identified as forged

FP (False Positive): Authentic image identifies as forged

TN (True Negative): Authentic image identified as authentic

FN (False Negative): Forged image identified as authentic

Further we define some parameters to measure the performance of the system [22]. They are as follows:

$$Sensitivity = \frac{TP}{TP + FN}$$

(1)

$$Specificity = \frac{TN}{TN + FP}$$
(2)

$$Specificity = \frac{TN}{TN + FP}$$
(3)

$$Accuracy = \frac{TP + TN}{TN + FP + TP + FN}$$
(4)

$PPV = \frac{TP}{TP + FP}$ (PPV: Positive Predictive Value)
(5)

$NPV = \frac{TN}{TN + FN}$ (NPV: Negative Predictive Value)
(6)

$FPR = 1 - specificity$ (FPR: False Positive Rate)
(7)

$FNR = 1 - sensitivity$ (FNR: False Negative Rate)
(8)

Sensitivity relates to the ability of the algorithm to detect a forged image correctly as forged. Specificity relates to the ability of the algorithm to identify an authentic image correctly as authentic. Hence a high value of sensitivity and specificity imply better performance of the system. Harmonic mean (which is the harmonic mean of sensitivity and specificity, as the name suggests) is also calculated. The results recorded are presented in Table I, Table 2 and Table 3.

As we can see the system achieves better performance when trained with both HMM and SVM. The overall accuracy, sensitivity and specificity improve. The same is demonstrated through the following graphs as shown in Figure 6 to Figure 9.

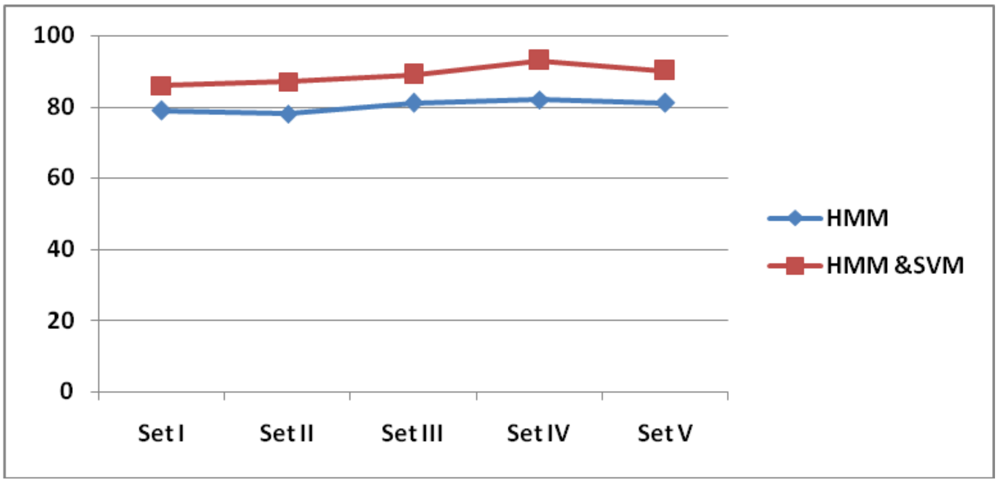

Figure 6. Accuracy Plot for HMM and HMM&SVM Systems

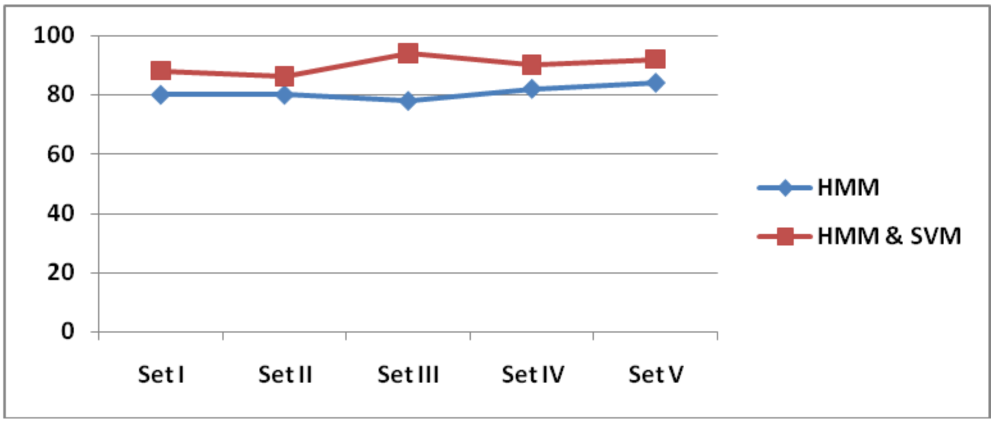

Figure 7. Sensitivity Plot for HMM and HMM&SVM Systems

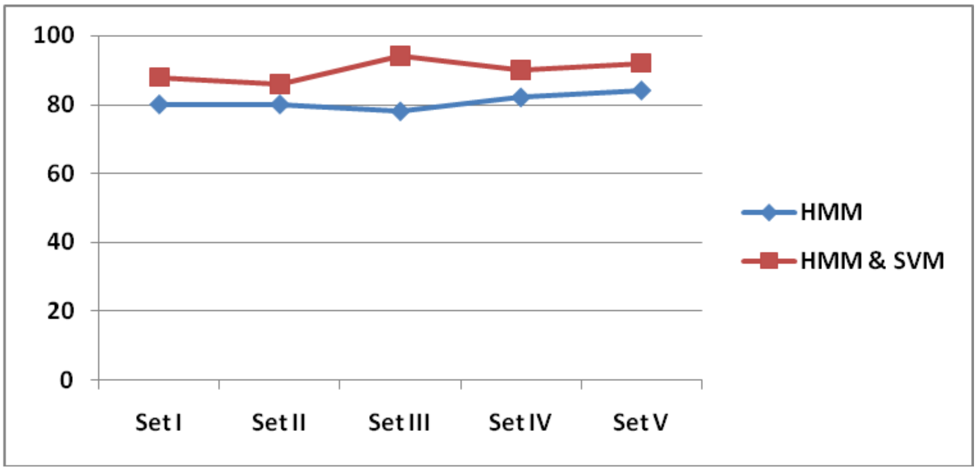

Figure 8. Specificity Plot for HMM and HMM&SVM Systems

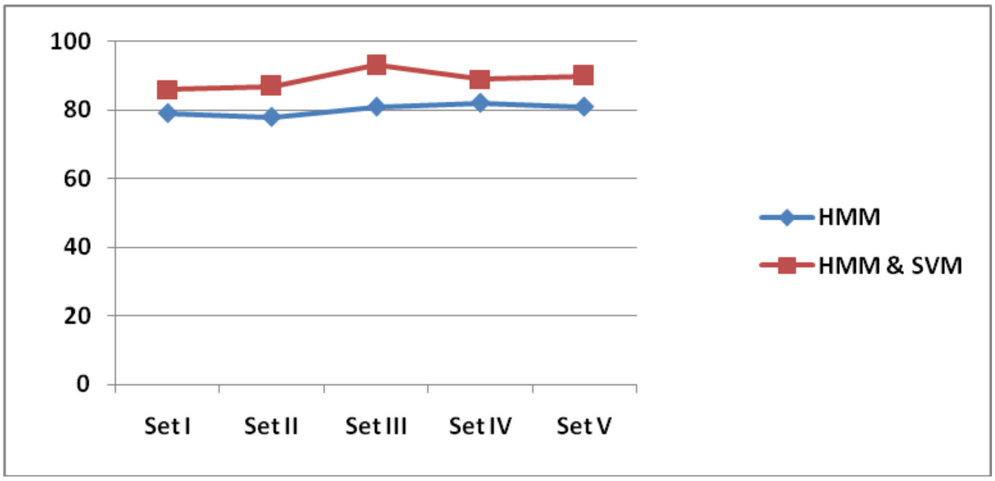

Figure 9. Harmonic Mean Plot for HMM and HMM&SVM Systems

Table 1. Calculation of Parameters of the System with HMM

Set	No. of authentic images	No. of forged images	TP	TN	FP	FN	Sensitivity (%)	Specificity (%)	Harmonic Mean (%)	Accuracy (%)
Set-I	50	50	40	39	11	10	80	78	78.98	79
Set-II	50	50	40	38	12	10	80	76	77.94	78
Set-III	50	50	39	42	8	11	78	84	80.88	81
Set-IV	50	50	41	41	9	9	82	82	82.00	82
Set-V	50	50	42	39	11	8	84	78	80.88	81
Total	250	250	202	199	51	48	80.80	79.60	80.19	80.20

Table 2. Calculation of Performance Parameters of the System with Hmm &SVM

Set	No. of authentic images	No. of forged images	TP	TN	FP	FN	Sensitivity (%)	Specificity (%)	Harmonic Mean (%)	Accuracy (%)
Set-I	50	50	44	42	8	6	88.0	84.0	85.95	86
Set-II	50	50	43	44	6	7	86.0	88.0	86.98	87
Set-III	50	50	47	46	4	3	94.0	92.0	92.98	89
Set-IV	50	50	45	44	6	5	90.0	88.0	88.98	93
Set-V	50	50	46	44	6	4	92.0	88.0	89.95	90
Total	250	250	225	220	30	25	90.0	88.0	88.98	89.0

Table 3. Calculation of Other Performance Parameters

Method	PPV(%)	NPV(%)	FPR (%)	FNR(%)
HMM	79.84	80.56	20.40	19.20
HMM & SVM	88.23	89.79	12.00	10.00

It has to be noted that the training set for modeling HMM and SVM was the same. We further compared the results of our work with the work of others. Comparison was done on the basis of system parameters which have been defined above. The following Table 4 gives the details of the same.

Table 4.Comparison of Proposed Method with Other Exiting Algorithms

Methods	Sensitivity (%)	Specificity (%)	Harmonic Mean (%)	Accuracy (%)
Lukàs-2006	66.93	90.93	77.81	91.82
Mahdian-2008	37.84	82.09	51.80	80.21
Farid-2009	37.70	90.0	53.14	87.80
Li-2009	91.59	45.24	60.56	47.21
Bianchi-2011	59.29	95.17	73.07	93.65
Proposed Method	**90.00**	**88.00**	**88.98**	**89.00**

As is evident from the above table, only Li [23] was able to manage a sensitivity of above 90%. However this is achieved at the cost of a very low specificity (below 50 %). Lukàs-2006[24] provided a good value of specificity and accuracy with an acceptable value of sensitivity.Bianchi-2011[25] provides a high specificity and accuracy. However the sensitivity achieved is less. Same is the case with Mahdian-2008[26]. Farid-2009 achieves a high specificity and accuracy [27]. However the sensitivity is very low (less than 40%). However the proposed method (system trained with both HMM and SVM) provides reasonable values for all parameters. All obtained values are above 85 %. Accuracy obtained is 89%. Sensitivity and Specificity for the proposed method are 90% and 88% respectively. Hence the proposed method has greater ability to detect a forged image as forged and to identify an authentic image as authentic. A comparative Bar-chart is shown in Figure 10.

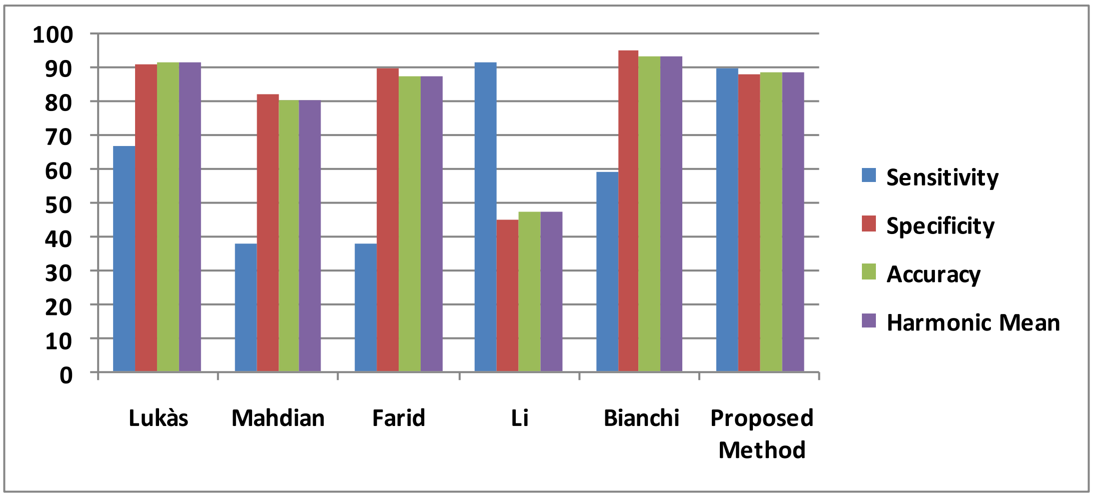

Figure 10. Comparison of Other Algorithms with the Proposed Method

8. Conclusion

The need for image forgery detection was felt since the invention of photography to establish the validity of the image. HMM and SVM classifiers were used in the proposed method. The digital image was represented by its feature vector in the transformed domain. LBP, Curvelet transform, DCT and Gabor filter were used for extracting features. We first tested the system performance with the system being trained only with the HMM model and then with SVM as well. It was found that system performance improved when it had been trained with both the models. Accuracy in case of the system trained with just HMM was found to be 80.20%. Accuracy in case of the system trained with both HMM and SVM was found to be 89. Further, the proposed method was compared to the existing methods. It was concluded that all the existing methods gave high value of one system parameter, at the cost of some other system parameter. The proposed method was however found to give reasonable values of all the system parameters (>85%). Overall accuracy was found to be 89%. Sensitivity and Specificity were found to be 90% and 88% respectively.

Acknowledgements

The authors would like to thank the coordinators of CoE, VNIT Nagpur for their valuable financial assistance. They also extend special thanks to Director, VNIT Nagpur for providing them with the needed administrative support. These should be brief and placed at the end of the text before the references.

References

[1] B. L. Shivakumar and S. S. Baboo, "Detecting copy-move forgery in digital images: a survey and analysis of current methods", Global Journal of Computer Science and Technology, vol. 10, no. 7, **(2010)**, pp. 61-65.

[2] Z. W. He, W. Lu, W. Sun and J. Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain", Pattern Recognition, vol. 45, no. 12, **(2012)**, pp. 4292-4299.

[3] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling", IEEE Transactions on Signal Processing, vol. 53, no. 2, **(2005)**, pp.758-767.

[4] F. Zach, C. Riess and E. Angelopoulou, "Automated Image Forgery Detection through Classification of JPEG Ghost", Proceeding of the Pattern Recognition, **(2012)**.

[5] H. C. Hsu and M. S. Wang, "Detection of copy-move forgery image using Gabor descriptor", Proceedings of the IEEE International Conference on Anti-Counterfeiting, Security and Identification (ASID), **(2012)**.

[6] L. Li, S. Li, H. C. Zhu, S. C. Chu, J. F. Roddick and J. S. Pan, "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, **(2013)**, pp. 15-56.

[7] M. Qiao, A. Sung, Q. Z. Liu and B. Ribeiro, "A novel approach for detection of copy-move forgery", Proceedings of the 5th International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP), **(2011)**.

[8] S. Khan and A. Kulkarni, "Detection of copy-move forgery using multiresolution characteristic of discrete wavelet transform", Proceedings of the ACM International Conference & Workshop on Emerging Trends in Technology (ICWET), TCET, **(2011)**;Mumbai, India.

[9] J. A. Fridrich, D. B. Soukal and J. A. Lukáš, "Detection of copy-move forgery in digital images", Proceedings of Digital Forensic Research Workshop, **(2003)**.

[10] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, **(2011)**, pp.1099-1110.

[11] E. S. Gopi, N. Lakshmanan, T. Gokul, S. K. Ganesh and P. R. Shah, "Digital image forgery detection using artificial neural network and auto regressive coefficients", Proceeding of the IEEE Canadian Conference on Electrical and Computer Engineering, (CCECE), **(2006)**.

[12] J. Edson, R. Justino, F. Bortolozzi and R. Sabourin, "A comparison of SVM and HMM classifiers in the off-line signature verification", Pattern Recognition Letters, vol. 26, no. 9, **(2005)**, pp. 1377-1385.

[13] S. Impedovo and M. G. Lucchese, "Improving a bank-check processing system with new HMM-based algorithms", Proceedings of the 5th WSEAS International Conference on Applied Informatics and Communications, **(2005)**; Malta.

[14] P. Sutthiwan, Y. Q. Shi, J. Dong, T. Tan and T. T. Ng, "New developments in color image tampering detection", Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), **(2010)**.

[15] J. Li, A. Najmi and R. M. Gray, "Image classification by a two-dimensional hidden Markov model", IEEE Transactions on Signal Processing, vol. 48, no. 2, **(2010)**, pp.517-533.

[16] CASIA Tampering Detection Dataset V1.0, **(2009)**.

[17] J. Fierrez, J. O. Garcia, D. Ramos and J. G. Rodriguez, "HMM-based on-line signature verification: Feature extraction and signature modeling", Pattern recognition letters, vol. 28, no. 16, (**2007)**, pp. 2325-2334.

[18] L. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition", Proceedings of the IEEE, **(1989)**.

[19] L. R. Rabiner and B. H. Juang, “Fundamentals of speech recognition”, 14. Englewood Cliffs: PTR Prentice Hall, **(1993)**.

[20] S. A. Daramola and T. S. Ibiyemi, "Offline signature recognition using hidden markov model (HMM)", International Journal of Computer Applications, vol. 10, no. 2, **(2010)**, pp. 17-22.

[21] C. C. Chang and C. J. Lin, LIBSVM: A Library for Support Vector Machines.

[22] D. Cozzolino, F. Gargiulo, C. Sansone and L. Verdoliva, "Multiple Classifier Systems for Image Forgery Detection", Proceedings of the Image Analysis and Processing (ICIAP), **(2013)**.

139

[23] W. H. Li, Y. Yuan and N. H. Yu. "Passive detection of doctored JPEG image via block artifact grid extraction", Signal Processing, vol. 89, no. 9, **(2009)**, pp. 1821–1829.

[24] J. Lukáš, J. Fridrich and M. Goljan, "Detecting digital image forgeries using sensor pattern noise", Proceedings of the SPIE, Electronic Imaging, International Society for Optics and Photonics, **(2006)**.

[25] T. Bianchi, A. De Rosa and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images", Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), **(2011)**.

[26] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation", IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, **(2008)**, pp. 529-538.

[27] H. Farid, "Exposing digital forgeries from JPEG ghosts", IEEE Transactions on Information Forensics and Security, vol. 4, **(2009)**, pp. 154-160.

[28] M. Pietikäinen, A. Hadid, G. Zhao and T. Ahonen, "Local binary patterns for still images", Computer Vision Using Local Binary Patterns, Computational Imaging and Vision, Springer-Verlag London Limited, **(2011)**, pp. 13-47.

[29] S. Bayram, H. T. Sencar and N. Memon, "A survey of copy-move forgery detection techniques", Proceedings of the IEEE Western New York Image Processing Workshop, **(2008)**.

[30] L. Demanet, CurveLab, vol. 2, no. 1, **(2008)**, p. 2.

[31] A. M. Deris, A. M. Zain and R. Sallehuddin, "Overview of support vector machine in modeling machining performances", Proceeding of the International Conference on Advances in Engineering (ICAE), Procedia Engineering, **(2011)**.

[32] S. J. Ryu, H. Y. Lee, I. W. Cho and H. K. Lee, "Document forgery detection with SVM classifier and image quality measures", Proceeding of the Advances in Multimedia Information Processing (PCM), **(2008)**.

Authors

Mohammad Farukh Hashmi received his B.E in Electronics & Communication Engineering from R.G.P.V Bhopal University. He obtained his M.E. in Digital Techniques & Instrumentation in 2010 from R.G.P.V Bhopal University. He is a member of IAENG. He is currently pursuing his doctoral studies at VNIT Nagpur under the supervision of Dr.A.G.Keskar. He has published up to 34 papers in international conferences and journals. He has a teaching experience of 3.5 years. His current research interests are Computer Vision, Embedded System, Circuit Design, Image Processing and Digital IC Design etc. Mr. Mohammad F. Hashmi is a member of IEEE, ISTE, and IAENG.

Avinash G. Keskar completed his B.E. from VNIT, Nagpur in 1979 and received gold medal for the same. He completed his M.E. from IISc, Bangalore in1983, receiving the gold medal again. The author is a member of IAENG. He has 26 years of teaching experience and 7 years of industrial experience. He is currently a PROFESSOR at Department of Electronics Engineering, VNIT Nagpur. His current research interests include Computer Vision, Soft Computing, and Fuzzy Logic etc. Dr. A. G. Keskar is a senior member of IEEE, FIETE, LMISTE, FIE**.**