Image tampering detection using genetic algorithm

Ritu Agarwal*, and *Mallika* Pant

Department of Information Technology, Delhi Technological University, New Delhi - 110042, India

Abstract. As digital images become an indispensable source of information, the authentication of digital images has become crucial. Various techniques of forgery have come into existence, intrusive, and non-intrusive. Image forgery detection hence is becoming more challenging by the day, due to the unwavering advances in image processing. Therefore, image forensics is at the forefront of security applications aiming at restoring trust and acceptance in digital media by exposing counterfeiting methods. The proposed work compares between various feature selection algorithms for the detection of image forgery in tampered images. Several features are extracted from normal and spliced images using spatial grey level dependence method and many more. Support vector machine and Twin SVM has been used for classification. A very difficult problem in classification techniques is to pick features to distinguish between classes. Furthermore, The feature optimization problem is addressed using a genetic algorithm (GA) as a search method. At last, classical sequential methods and floating search algorithm are compared against the genetic approach in terms of the best recognition rate achieved and the optimal number of features.

1 Introduction

In today's era of digitalization and computerization, information is mostly conveyed through digital images and videos. Fields like weather forecasting, forensic investigation, journalism have raised the need for digital images. Due to the increase in the availability of a wide range of image-editing software and advancement in processing techniques, image forgery is on the rise and thereby effecting diverse areas of life, such as politics, cybercrime investigations, medical diagnoses based on images, politics, businesses etc. Crimes, such as defaming of websites, personalities etc., are on the rise and make use of such tools to do the act. Different type of forging techniques has come up of which, Image Splicing is performed by cutting and merging more images and is common among all. Copy move forgery is another forgery technique, detection of which by human visual system is very difficult. In this type of forgery, a part of an image is replicated in the same image in another region that depicts as an authenticated image.

Although, Human visual system has difficulty in perceiving spliced images and copy move forged images. New and efficient methods to detect forgery in images are proposed

* Corresponding author: ritu.jeea@gmail.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

by researchers. The available techniques for tampering detection can be divided into broadly into active approaches [1][2] and passive approaches [3][4]. The former needs addition of traces of authenticity to be able to detect later for any manipulations, for example a digital watermark where we feed some information prior to image sharing and the detection can be done based on modifications to that information, whereas the passive approaches use a blind approach, perform the same task without any prior information. They make use of the distinct properties of original images and traces of changes made to them to perform authentication. The proposed method uses a blind approach to find out whether the given image is altered or not.

2 Digital image forgery detection methods

2.1 Active approach

Active forgery detection approaches [1][2] use a digital watermark or a signature embedded in the actual image to prove or reject the authenticity of the image. This approach holds a strong limitation that the watermark which is embedded must be performed either by a person authorized to process the image or by the acquisition device.

2.2 Passive approach

Passive/Blind approaches [3][4] use the fact that statistical changes occur in images or camera fingerprints during the process of creation/modification, to detect the forgery. Unlike active methods, blind approaches do not require any data regarding authenticity. Blind forensics can be classified into six categories [5] i.e. pixel-based, camera based, format-based, geometric-based, physics-based and source camera identification-based.

3 Related work

Image splicing detection detects if a given image is a composite one created by combining or separating different portions of two or more images. Copy move forgery detects if an image contains a copied portion of the same image. In a series of paper [6] [7] higher order moment spectra, bi-coherence are treated as features in order to detect images that are spliced. When tested, bi-coherence was found sensitive to quadratic phase coupling. The accuracy of 72% was found when these features are performed on a dataset. A combination of Hilbert Huang Transform and wavelet decomposition [8] is proposed in which Hilbert Huang Transform is used to examine disturbance in linearity caused by image splicing and a statistical model using wavelet decomposition is proposed for calculating moments of the characteristic function. Detection accuracy was 80.15% was found when these two features were used collectively. Hsu and Chang [9] used camera response function and geometry invariants to detect splicing in a semi-automatic manner. In order to automate their work, image segmentation is incorporated [10]. The measure of blurriness [11] and local sharpness [12] was taken as an advantage to check if image under detection is blurred/smoothed or not. A scheme to detect a tampered region in JPEG images was proposed in [13]. In [14] a scheme used for steganalysis was used to check image splicing. He et al. used Run- Length based scheme to detect forgery [15]. Statistical moments obtained from wavelet characteristic function and 2D phase congruency [16] were used to pull out spliced ones from original ones. On detection of these features on Columbia Image Splicing Evaluation Dataset [17] using SVM classifier, an accuracy of 82.32% was attained. Shi et al [18] checked two different types of statistical features proposing a natural image

model on Columbia Image Splicing Dataset attaining detection accuracy of 91.87%. In [19] presented an algorithm for tampering detection using SVD. A small window of size B x B is slid over the input image to separate the image into overlapping blocks. SVD is applied to these separated blocks to obtain feature vectors, sort them and store it in the matrix. k-d tree is constructed using the feature vectors and it is searched for similar blocks. The matched blocks satisfying a threshold t will be labeled as suspected regions and these suspected regions are merged together to determine the tampered region. With the above discussion, we can conclude that there are several methods for locating the altered region.

4 Proposed approach

The approach starts by extracting features from given input images. To achieve a high recognition rate, a subset of best features need to be selected. Exhaustive search to evaluate best feature subset is not feasible as it increases required computational effort. The genetic approach, being a heuristic search provide a feasible approach for such an optimization problem and therefore used for feature selection in the proposed approach as shown in figure 1. Classical sequential methods are compared with genetic algorithm approach in context with recognition rate and cardinality of feature subset chosen.

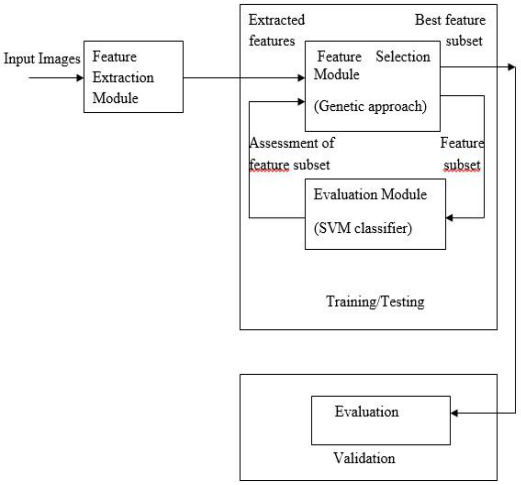

Fig. 1. The architecture of detection algorithm.

4.1 Feature Extraction

A set of ten features are pulled out from authentic as well as spliced images. They are:

4.1.1 Local binary pattern

It is an efficient texture feature which works by labeling the pixels of an image and then thresholding each of the neighbors. Finally, the result is displayed as a binary number.

4.1.2 Entropy

$$ENT = -\sum_{i=1}^{N}\sum_{j=1}^{N} C(i,j)\log\left(C(i,j)\right) \quad (1)$$

where C denotes the co-occurrence matrix and N is the number of levels that are gray in the quantized image.

4.1.3 Contrast

$$CON = \sum_{n=0}^{N-1} n^2 \left\{ \sum_{i=1}^{N} \sum_{j=1}^{N} \{C(i,j)\} \right\} \quad (2)$$

4.1.4 Histogram of oriented gradients (HOG)

These descriptors use the fact that the occurrences of gradient orientation help to localize the parts in the image. Unlike SIFT, it performs on dense grid structure of cells spaced uniformly. It performs local contrast normalization on blocks that are overlapped.

4.1.5 Inverse difference moment

$$IDM = \sum_{i=1}^{N} \sum_{J=1}^{N} \frac{1}{1+(i-j)^2} C(i,j) \quad (3)$$

4.1.6 Speeded up robust features

It uses the multi-resolution pyramid technique to extract features in images which are transformed into coordinates.

4.1.7 Inertia

$$INER = \sum_{i=1}^{N} \sum_{j=1}^{N} (i-j)^2 * C(i,j) \quad (4)$$

4.1.8 Cluster shade

$$CS = \sum_{i=1}^{N} \sum_{j=1}^{N} \left(i + j - u_x - u_y\right)^3 * C(i,j) \quad (5)$$

4.1.9 Cluster prominence

$$CP = \sum_{i=1}^{N} \sum_{j=1}^{N} \left(i + j - u_x - u_y\right)^4 * C(i,j) \quad (6)$$

4.1.10 Angular second moment

$$ASM = \sum_{i=1}^{N} \sum_{j=1}^{N} \{C(i,j)\}^2 \quad (7)$$

4.2 Feature Selection

Feature selection is done to use a smaller feature set while maintaining the accuracy of classification.

4.2.1 Deterministic search method

Feature selection algorithms are divided into the following categories, which are Exponential, randomized and sequential algorithms. The algorithms of sequential search use hill-climbing strategy to select or reject features. Sequential forward selection (SFS) starts by evaluating all feature subsets which contains one feature and select the feature with the best performance. This subset is then combined with the feature that gives the best performance for larger size subsets. The process repeats until no improvement is done by extending the current subset. Sequential backward selection (SBS) starts with a set which contains all features and repeatedly removes a feature whose rejection gives a maximal

improvement in performance. Both these methods are suboptimal methods that create nesting of features in a straight forward manner. Due to these previous additions and removal of features cannot be corrected. To overcome this problem, these algorithms are modified and are termed as floating sequential algorithms. Sequential floating forward selection (SFFS) works by applying backward steps after each forward step until the corresponding subsets are better than previous ones.

4.2.2 Genetic algorithm approach

In order to select the best set of features, a genetic algorithm which is based on global search method is used. Based on Darwin principle, the algorithm states that the initial population of individuals have a high probability of survival. Here each feature subset is encoded in form of a binary string which is called a chromosome. Each bit is associated with a feature in the binary vector. If the i^{th} bit of this vector is 1 then it means that i^{th} feature is allowed to participate in classification. In case the bit is a 0, then the feature is not selected. The fitness value is assigned based on classification performance. Here genetic approach has been used to select the best features by tournament approach. Diagnostic accuracy, sensitivity, and specificity measure are considered for evaluation. Also, the number of features that are not selected (zeros in a chromosome) with a coefficient is added.

Fitness function:

$$fitness = Accuracy + Sensitivity + Specificity + 0.05 * Number \quad (8)$$

In order to maintain diversity in solution, replacement technique is used and the whole population is replaced with the new generation. Parents having a high selection rate are selected. For simplicity, single point crossover is adopted here. The feature subset among all the generations with the highest classification rate is regarded as the optimum.

4.2.3 Classification

The proposed approach improves the usefulness of machine learning techniques that are used for classification. The main objective as a whole, is to improve the accuracy of classification and reduce the size of feature subsets using a genetic algorithm approach. To save time, the population size and the number of generations used by genetic algorithm are relatively small. To achieve better results, it is possible to allow more iterations or larger population size. SVM and Twin SVM [20] used as classifiers. SVM is a non-probabilistic supervised learning method which develops a model which assigns a class label based on patterns.

Twin SVM is a binary SVM classifier that solves two related SVM type problems and obtains two non-parallel planes. Both problems are smaller than in a standard SVM. The Twin SVM classifier is obtained by solving a pair of quadratic programming problems. For each class, it finds two hyperplanes and then classifies point. The first term in the objective function is the sum of squared distances from the hyperplane to points of one class. Therefore, minimizing it tends to keep the hyperplane close to points of one class. The second term of the objective function minimizes the sum of error variables. In short, Twin SVMs consists of a pair of quadratic programming problems. In each QPP, the objective function corresponds to a particular class and the constraints are determined by patterns of the other class. Twin SVM classify approximately four times faster than the usual SVM.

5 Results and discussion

The results are evaluated and determined for its accuracy, robustness, and computational complexity with respect to the proposed approach. For evaluation purposes, two datasets

are selected. One of them is the most commonly available dataset for splicing detection which is Columbia Image Splicing Detection [20]. It consists of 933 authentic and 912 spliced images with a size of 128 x 128 pixels. The second dataset named MICC – F220 [21] of 220 images is used, 110 images of which are forged images and 110 are originals. The image resolution range varies from 722 x 480 to 800 x 600 pixels. The dataset depicts alterations such as translation, rotation, scaling (symmetric/asymmetric) and/or a combination of these while copying and pasting. The database images are divided into subgroups for implementation issues.

5.1 Performance measures

Performance of an algorithm can be measured in terms of accuracy, sensitivity, and specificity as given in equation 8,9,10. Some of the few terms used in the calculation are:

TN (True negative): - Authentic image is detected as authentic only
FN (False negative): - Forged image is detected as authentic
TP (True positive): - Forged image detected
FP (False positive): - Authentic image is detected as forged

$$\text{Accuracy: } \frac{TP+TN}{TP+TN+FP+FN} \tag{8}$$

$$\text{Sensitivity: } \frac{TP}{TP+FN} \tag{9}$$

$$\text{Specificity: } \frac{TN}{TN+FP} \tag{10}$$

5.1.1 Performance measure on MICC-F220 [21] dataset

Given below some of the result in terms of Accuracy, Sensitivity, and Specificity as mentioned above on MICC-F220 dataset. table 1 and table 2 shows the difference between SVM, and Twin SVM classifier in terms of performance measure. The best chromosomes selected by the genetic algorithm based on the features extracted from the images is given on table 3.

Table 1. Performance parameters on MICC-F220 using SVM as classifier.

Image	Accuracy	Sensitivity	Specificity	Average
Tampered 1	93.33	100	85.71	93.01
Tampered 2	92.84	100	85.03	92.62
Tampered 3	93.33	100	85.71	93.01
Tampered 4	92.56	100	86.20	92.92

Table 2. Performance parameters on MICC-F220 using Twin SVM as a classifier.

Image	Accuracy	Sensitivity	Specificity	Average
Tampered 1	93.33	100	85.71	93.01
Tampered 2	92.84	100	85.03	92.62
Tampered 3	93.33	100	85.71	93.01
Tampered 4	92.56	100	86.20	92.92

Table 3. Best chromosomes selected by Genetic Algorithm for MICC-F220

Accuracy	Image name
93.33	HOG, LBP, CON
93.33	HOG, CON, IDM
92.45	LBP, SURF, CON
93.33	LBP, CS,INER
92.48	SURF,ENT,CS
93.02	HOG,LBP,CON,CS
92.65	HOG,LBP,CON,CP
91.87	HOG,SURF,INER,LBP
93.01	IDM,SURF,CS,ENT
91.67	IDM,ENT,LBP,CON

5.1.2 Performance measure on Columbia Dataset

Similar to MICC-F220 given below table 4, table 5 and table 6 gives a comparative comparison on Columbia dataset.

Table 4. Performance parameters on Columbia dataset using SVM as classifier.

Image	Accuracy	Sensitivity	Specificity	Average
Tampered 1	88.63	86.90	90.52	88.68
Tampered 2	88.63	86.95	90.47	88.68
Tampered 3	88.67	87.45	88.34	88.15
Tampered 4	88.67	87.56	88.45	88.22

Table 5. Performance parameters on Columbia dataset using Twin SVM as classifier.

Image	Accuracy	Sensitivity	Specificity	Average
Tampered 1	88.63	86.95	90.47	88.68
Tampered 3	86.57	89.47	88.65	88.36
Tampered 5	86.10	85.76	89.56	87.14
Tampered 11	88.63	86.95	90.47	88.68

Table 6. Best chromosomes selected by Genetic Algorithm in 10 iterations for Columbia dataset.

Accuracy	Image name
88.65	HOG, INER, CON
88.67	LBP, HOG, CS
89.56	HOG,INER,LBP
85.64	HOG, CS, CON
86.78	SURF,INER,CON
88.97	SURF,INER,CON,ENT
86.45	LBP,IDM,CON,HOG
85.64	LBP,SURF,CON,CS
85.78	HOG,LBP,CON,CS
86.76	ENT,SURF,IDM,CS

5.1.3 Comparative study

The same set of feature set belonging to MICC F220 and Columbia dataset when applied to classical feature selection algorithms like Sequential floating forward selection (SFFS), sequential backward selection (SBS), sequential forward selection (SFS), and like methods gave the following feature subset with the accuracy as shown below in table 7 and table 8:

Table 7. Performance parameters of sequential feature selection algorithms on MICC F220 dataset using SVM as a classifier.

Feature selection algorithm	Feature set algorithm	Accuracy
SFS	HOG,INER,CS,LBP	93.33
SBS	HOG, INER ,SURF,CS	93.33
SFFS	HOG,INER,LBP,CS	93.33

Table 8. Performance parameters of sequential feature selection algorithms on Columbia dataset using SVM as a classifier.

Feature selection algorithm	Feature set algorithm	Accuracy
SFS	HOG, CON, LBP, INER	88.63
SBS	LBP,IDM,CS, SURF	88.63
SFFS	LBP,CON,CS,HOG	88.63

The execution time of the algorithm using SVM and Twin SVM as classifier can be compared with the following graph as given in figure 2.

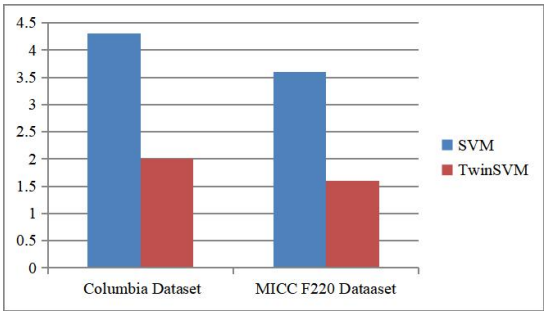

Fig. 2. The execution time of Twin SVM and SVM classifier.

6 Conclusion

This paper describes a technique to detect alteration in images with competing for accuracy and significantly low computational complexity and robust to various kinds of manipulations such as compression, rotation, scaling, etc. as can be seen from the database selection. As we know that different features of an image are used to detect different types of forgery accurately and efficiently. So a system is designed to collect the best of all features and classify them to detect forgery. To achieve this, set of ten features are selected and from them, the best of features are selected using genetic feature selection algorithm, which can further reduce the feature dimensions to get more optimal results. The reduced feature set is passed to SVM and Twin SVM for classification to get the final class results and the performance parameters are accuracy, sensitivity, and specificity. We obtain comparative results with a significant low computational complexity

References

1. C Rey and J-L Dugelay, "A survey of watermarking algorithms for image authentication.," *EURASIP Journal on Applied Signal Processing*, pp. 613-621, 2002.
2. V M Potdar, S Han, and E Chang, "A survey of digital image watermarking," in *3rd IEEE International Conference on Industrial Informatics*, Perth,WesternAustralia, 2005, pp. 709-716.
3. Granty Regina Elwin J, Aditya T S, and Madhu Shankar S, "Survey on Passive Methods of Image Tampering Detection," in *Proceedings of the International Conference on Communication and Computational Intelligence*, 2010, pp. 431-436.
4. B Mahdian and S Saic, "A bibliography on blind methods for identifying image forgery," in *Signal Processing:Image Communication*, 2010, pp. 389-399.
5. M Ali Qureshi and M Deriche, "A Review on Copy Move Image Forgery Detection Techniques," in *IEEE*, 2014.
6. T T Ng and S F Chang, "Blind Detection of Digital Photomontage using Higher," ColumbiaUniversity, 2004.
7. T T Ng and S F Chang, "A model for image splicing," in *IEEE International Conference on Image Processing*, Singapore, 2004, pp. 1169–1172.
8. D Fu, Y Q Shi, and W Su, "Detection of image splicing based on Hilbert–Huang transform and moments of characteristic functions with wavelet decomposition," *Lecture Notes in Computer*, vol. 4283, pp. 177–187, 2006.
9. Y F Hsu and F S Chang, "Detecting image splicing using geometry invariants and camera characteristics consistency," in *IEEE ICME*, Toronto,Canada, 2006, pp. 549–552.
10. F Y Hsu and S F Chang, "Image splicing detection using camera response function consistency and automatic segmentation," in *IEEE ICME*, Beijing, China, 2007, pp. 28–31.
11. Q Zheng, W Sun, and W Lu, "Digital spliced image forensics based on edge blur measurement," in *IEEE International Conference on Information Theory and Information Security*, Beijing,China, 2010, pp. 399–402.
12. Y Sutcu, B Coskun, H T Sencar, and N Memon, "Tamper detection based on regularity of wavelet transform coefficients," in *IEEE International Conference on Image Processing*, SanAntonio,TX,USA, 2007, pp. 397–400.
13. Z Lin, J He, X Tang, and C K Tang, "Fast automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," in *PatternRecognition*, 2009, pp. 2492–2501.
14. J Dong, W Wang, T Tan, and YQ Shi, "Run-length and edge statistics based approach for image splicing detection," *Lecture Notes in Computer Science*, pp. 76–87, 2009.
15. Z He, W Sun, W Lu, and H Lu, "Digital image splicing detection based on approximate run length," in *Pattern Recognition Letters*, 2011, pp. 1591–1597.
16. W Chen, Y Q Sh, and W Su, "Image splicing detection using 2-D phase congruency and statistical moments of characteristic function," in *Imaging Security, Steganography,andWatermarking of Multimedia Contents*, 2007.
17. Ng and S F Chang, "A DataSet of Authentic and Spliced Image Blocks," Columbia University, Technical Report 2004.
18. Y Q Shi, C Chen, and W Chen, "A natural image model approach to splicing detection," in *MM & Sec*, Dallas,TX,USA, 2007, pp. 51–62.
19. S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," 2016 *IEEE International Conference on Recent Trends in*

Electronics, Information & Communication Technology (RTEICT), Bangalore, 2016, pp. 706-710.

20. Jayadeva , R Khemchandani, and Suresh Chandra, "Twin Support Vector Machines for Pattern Classification," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE,* vol. 29, pp. 905-910, MAY 2007.
21. Amerini, Irene, Lamberto Balian, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe 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 ,pp. 1099-1110, 2011.