International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Hybrid Feature Classification Model with Probabilistic Classification of the Image Forgery Detection

Samiksha Singla[1], Harpreet Tiwana[2]

[1, 2]Doaba Group of Colleges, Punjab, India

Abstract: ***The image forgery detection is the technique to find the forgery in the images by analyzing the image matrix against the ground truth image. The image forgery detection plays the very important role for the digital media houses. The image data theft or copyright forgery may cause the hefty monetary losses to the real owners of the digital image data. To protect the copyright of the real owner, the image forgery methods are incorporated over the suspected image data. Several factors are analyzed under the proposed model in order to recognize the real identity of the image, which is decided in the terms of authentic or forged image. In this paper, the proposed model has been designed with the multiple features based image forgery evaluation. The incorporation of the fast retina key points (FREAK) along with the speeded up robust features (SURF) have been utilized for the development of the robust feature descriptor. The support vector machine (SVM) has been used for the probabilistic classification of the model. The experimental results have been obtained in the form of statistical parameter after the testing under the various numbers of test cases. The experimental results have clearly defined the proposed model as the winner in comparison with the existing models***.

Keywords: Forgery detection, hybrid classification, robust classification, robust feature descriptor

1. Introduction

Authenticating digital images is a very serious issue and so far the researchers developed many methods, which can mainly be classified into (1) intrusive (active) and (2) non-intrusive (blind or passive) techniques . Further, intrusive methods can be divided into two classes based on (1) embedding a watermark and (2) incorporating digital signature in an image. In each of these techniques, a piece of information is integrated into digital images as an aid for authenticating digital contents and security rights.

Once the digital contents of an image are changed, the incorporated information is also modified. The authenticity of an image is validated by ensuring that the embedded information is unaltered. Though these methods are robust, their domain of application is restricted because all digital cameras are not equipped with the feature of embedding digital signature. In addition, these methods need pre-processing for creating labeled images. These limitations and constraints of active methods motivated the research to propose non-intrusive methods for authenticating digital images. This class of methods do not take into consideration any kind of embedded information (such as watermarks or signatures) to validate the authenticity of a digital image. Instead, these methods draw their conclusions about the originality of the digital content of images using its structural changes, which take place due to tempering.

The development of computer technology has enabled digital image forgery extremely easy and leaves no visual clue of being tampered. This fact is deteriorating the historical trust of image evidences. In digital investigation, there are active and passive ways to authenticate integrity of digital images. Active techniques involve embedding of data during the time of recording or sending. Digital watermarks and digital signatures are widely used active image authentication techniques. However, it is not always feasible to embed a watermark or signature to an image. This limits the use of active techniques. Passive authentication techniques are based on the analysis of different image attributes to detect inconsistencies that might be caused by forgery. Different features of image can be used for forgery detection, pixel statistics of natural image, lossy compression artifacts, the nature of image capturing devices, and the characteristics of interaction between physical object, light and camera and so on.

One of the main features of our daily experience is the ability to distinguish between things, to identify them and to link them with our prior knowledge. This ability to recognize and interpret the environment around us, is in principle the foundation for any higher level of processing that we do. Synonymous is the concept of clustering, segmentation and classification in artificial intelligence. Inspired by the working of human brain, the conception of learning algorithms took birth. These algorithms in essence provide us with a methodology to find parameters which would be able to identify and classify different objects in a given signal input. Researchers, in general have looked at different aspects of the brain like vision, hearing, speech etc for a better understanding of their functioning and in an attempt to model these processes.

We consider here a fundamental problem of computer vision, i.e. enabling computers to see the way we see things. We in future wish our machines would match the capabilities of human vision. Its interesting to note that, every second we receive tremendous amount of visual data and almost unconsciously we process this information very quickly. Classifying an object as table, a ball, or a scene as mountain or river is pretty trivial for us. We can in fact process amazingly more complex information. Its a well known fact that robotic vision compares miserably with our eyes. Here, we intend to make a start towards our goal by considering a very trivial problem by the standard of human vision and that is scene classification. Given an image of the scene we wish to classify it as say a mountain, forest, city, street etc.

Licensed Under Creative Commons Attribution CC BY

2. Related Work

2014. Li, Jian [1] has proposed the segmentation-based Image Copy-move Forgery Detection Scheme. In this paper, the authors have proposed a scheme to detect the copy-move forgery in an image, mainly by extracting the keypoints for comparison. The main difference to the traditional methods is that the proposed scheme first segments the test image into semantically independent patches prior to keypoint extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process consists of two stages. In the first stage, they have found the suspicious pairs of patches that may contain copy-move forgery regions, and roughly estimated an affine transform matrix. In the second stage, an Expectation-Maximization-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy-move forgery.

2014. Hashmi, Mohammad Farukh [11] has worked on the copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. In this paper, the authors have proposed a series of algorithms which are combination of speeded-up robust feature transforms and Wavelet Transforms. In doing so authors have first discussed the Speeded-Up Robust Feature (SURF), SURF in combination with Discrete Wavelet Transform (DWT), SURF in combination with Dyadic Wavelet Transform (DyWT). These algorithms are different from the previously proposed algorithm in the manner that they are applied on the entire image to extract features rather than dividing the image into the blocks. From the results obtained they are able to conclude the proposed algorithms are better than their counterparts both in terms of computational complexity and invariance to scale and rotation and also for the combination of attacks.

2014. Ayalneh, Dessalegn et. al. [3] have proposed the JPEG copy paste forgery detection using BAG optimized for complex images.

Image forgery detection is one of important activities of digital forensics. Forging an image has become very easy and visually confusing with the real one. Different features of an image can be used in passive forgery detection. Most of lossy compression methods demonstrate some distinct characteristics. JPEG images have a traceable zero valued DCT coefficients in the high frequency regions due to quantization. This appears as a square grid all over the image, known as Block Artifact Grid (BAG). In this paper the BAG based copy-paste forgery detection method is improved by changing the input DCT coefficients for Local Effect computation. The proposed method has shown a better performance especially for complex images.

2014. Hussain, Muhammad [4] has performed a performance evaluation survey on WLD and LBP descriptors for non-intrusive image forgery detection. The authors have investigated the detection of copy-move and splicing, the two harmful types of image forgery, using textural properties of images. Tampering distorts the texture micro-patterns in an image and texture descriptors can be employed to detect tampering. They did comparative study to examine the effect of two state-of-the-art best texture descriptors: Multiscale Local Binary Pattern (Multi-LBP) and Multiscale Weber Law Descriptor (Multi-WLD). Multiscale texture descriptors extracted from the chrominance components of an image are passed to Support Vector Machine (SVM) to identify it as authentic or forged.

2014. Jaberi, Maryam et. al. [5] has worked with accurate and robust localization of duplicated region in copy–move image forgery. In this paper, the authors have adopted keypoint-based features for copy-move image forgery detection; however, our emphasis is on accurate and robust localization of duplicated regions. In this context, we are interested in estimating the transformation (e.g., affine) between the copied and pasted regions more accurately as well as extracting these regions as robustly by reducing the number of false positives and negatives. To address these issues, they have proposed using a more powerful set of keypoint based features, called MIFT, which share the properties of SIFT features but also are invariant to mirror reflection transformations. Moreover, they have also proposed refining the affine transformation using an iterative scheme which improves the estimation of the affine transformation parameters by incrementally finding additional keypoint matches. To reduce false positives and negatives when extracting the copied and pasted regions, they propose using “dense” MIFT features, instead of standard pixel correlation, along with hystereresis thresholding and morphological operations.

2014. Muhammad, Ghulam [6] have developed an image forgery detection technique using steerable pyramid transform and local binary pattern. In this paper, a novel image forgery detection method is proposed based on the steerable pyramid transform (SPT) and local binary pattern (LBP). First, given a color image, the authors transform it in the YCbCr color space and apply the SPT transform on chrominance channels Cb and Cr, yielding a number of multi-scale and multi-oriented subbands. Then, they describe the texture in each SPT sub band using LBP histograms.

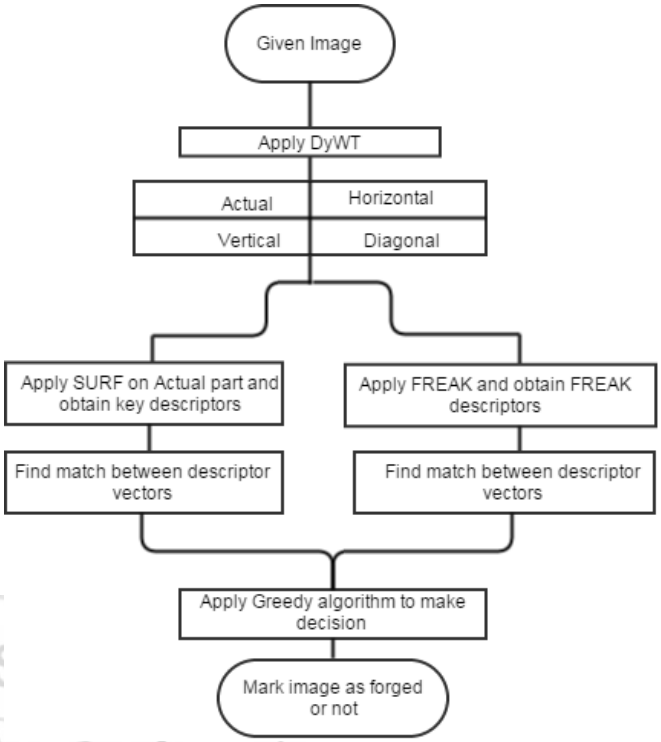
Licensed Under Creative Commons Attribution CC BY

3. Experimental Design

The proposed model is entirely based upon the incorporation of the various feature descriptors altogether for the purpose of image forgery detection. The popular feature descriptors of speeded up robust features (SURF) and fast retina key points (FREAK) has been established under this simulation scenario. The incorporation of the multiple features adds the robustness to the proposed model design, which has increased the accuracy of the overall system in detecting the image forgery. The proposed model approach with hybrid features has been further infused with the support vector machine (SVM) based probabilistic classification algorithm. The proposed model design has been elaborated in the following section:

Algorithm 1: Hybrid Feature based Image Forgery Detection Method

1. Submit the target image
2. Acquire the image matrix
3. Get the image size in number of rows and columns
4. Check if the image is 3-D by checking the depth of image defined in the 3rd dimension of size array.
5. If image is found 3-D
   a. Perform the matrix grayscale conversion
6. Prepare the test data
   a. Apply the SURF feature descriptor over the image matrix
      1. Return the key-point information array
   b. Apply the FREAK feature descriptor over the image matrix
      1. Return the key-point information array
7. Load the training data
   a. Load the pre-defined feature descriptor matrix containing the forged and authentic images.
8. Reconstruct the SURF feature descriptor matrix according to the size of training data
9. Reconstruct the FREAK feature descriptor matrix according to the size of training data
10. Perform the SVM classification over the SURF data
    a. Return the decision logic over SURF data (Decision 1)
11. Perform the SVM classification over the FREAK data
    a. Return the decision logic over FREAK data (Decision 2)
12. If decision 1 and decision 2 returns the similar results
    a. Mark the input image accordingly
13. Otherwise
    a. Return the freak result as final result



4. Result Analysis

The results of the proposed model have been analyzed from the input test size of 100 samples. The testing samples are randomly selected from the test input repository defined in the proposed model. The image are acquired and tested one after one in the iterative manner in order to evaluate the collaborated results from the input test data. The statistical measures have been evaluated in the initial stage, where the statistical errors of category 1 and 2 are evaluated. The category 1 and 2 measures includes the positivity and negativity based results from the proposed model.

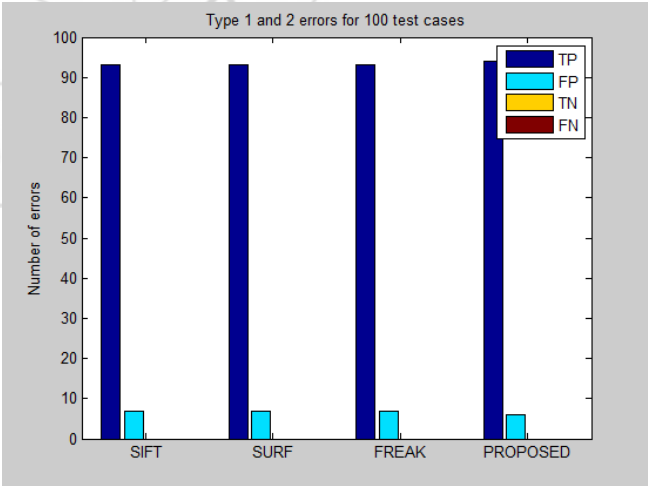


Figure 4.1: Type 1 and type 2 errors for 100 test cases

In the above figure 4.1, the statistical category measures have been defined for the all of the tested samples with different feature descriptors and the support vector machine (SVM). The proposed model has been recorded with the higher true positive cases than all other candidates and lower false alarms. The less false alarms and the higher number of true

Licensed Under Creative Commons Attribution CC BY

positive cases defines the robustness of the proposed model. The following figure 4.2 shows the statistical parameteric results obtained from the simulation:

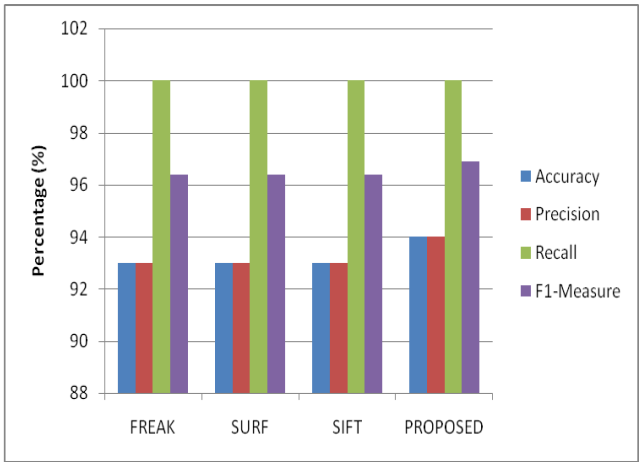


Figure 4.2: Performance measures for 100 test cases

The figure 4.2 represents the results obtained from all of the incorporated models, where the proposed model is found to be better than the other in the terms of precision, overall accuracy and f1-measure. The proposed model has been remained equal performer in the accordance to the existing models on the basis of the recall parameter, which clearly shows that the proposed model has not produced any extra false negative cases.

Table 4.1: Performance measures for 100 test cases

	FREAK	SURF	SIFT	PROPOSED
Accuracy	93	93	93	94
Precision	93	93	93	94
Recall	100	100	100	100
F1-Measure	96.37306	96.37306	96.37306	96.90722

The table 4.1 depicts the performance measure obtained after the performance evaluation of the proposed model and other models in our research. The testing models have defined the clear difference of the proposed model against the existing models in the terms of accuracy, precision and f1-measure.

5. Conclusion

The proposed model has been designed by infusing the textural feature descriptors. The textural feature descriptors utilized in the proposed model includes the difference of hessian based matrix evaluation and strong point extraction, where the other feature descriptor is evaluated on the basis of the binary mask or binary feature. The difference of hessian based feature descriptor known as speeded up robust feature (SURF) along with the binary feature descriptor fast retina key points (FREAK) have been infused for the realization of the robust feature descriptors. The proposed model has undergone various testing paradigms, where the proposed model has been found the best performer among all of the other feature descriptors. The F1-measure of 96.90 has been recorded against the maximum of 96.37 in the existing models, whereas the 94% overall accuracy has been recorded against the 93% obtained from the other descriptors

References

[1] Li, Jian, Xiaolong Li, Bin Yang, and Xingming Sun. "Segmentation-based Image Copy-move Forgery Detection Scheme.", Information Forensics and Security, IEEE Journals, 2014.

[2] Hashmi, Mohammad Farukh, Vijay Anand, and Avinash G. Keskar. "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms." In *Computer and Communication Technology (ICCCT), 2014 International Conference on*, pp. 147-152. IEEE, 2014.

[3] Ayalneh, DessalegnAtnafu, HyoungJoong Kim, and Yong Soo Choi. "JPEG copy paste forgery detection using BAG optimized for complex images." In*Advanced Communication Technology (ICACT), 2014 16th International Conference on*, pp. 181-185. IEEE, 2014.

[4] Hussain, Muhammad, Sahar Q. Saleh, HatimAboalsamh, Ghulam Muhammad, and George Bebis. "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection." In *Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 2014 IEEE International Symposium on*, pp. 197-204. IEEE, 2014.

[5] Jaberi, Maryam, George Bebis, Muhammad Hussain, and Ghulam Muhammad. "Accurate and robust localization of duplicated region in copy–move image forgery." *Machine vision and applications* 25, no. 2 (2014): 451-475.

[6] Muhammad, Ghulam, Munner H. Al-Hammadi, Muhammad Hussain, and George Bebis. "Image forgery detection using steerable pyramid transform and local binary pattern." *Machine Vision and Applications* 25, no. 4 (2014): 985-995.

[7] E. Ardizzone, A. Bruno, and G. Mazzola, "Detecting multiple copies in tampered images." In Proceedings of the 17th IEEE International Conference on Image Processing (ICIP -10), pp.2117–2120, September 2010.

[8] Zhang, Chenyang, XiaojieGuo, and Xiaochun Cao. "Duplication localization and segmentation." In Proceedings of Advances in Multimedia Information Processing(PCM 2010), pp. 578-589, Springer Berlin Heidelberg, 2010.

[9] Amerini, Irene, LambertoBallan, 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.

[10] Hashmi, Mohammad Farukh, Aaditya R. Hambarde, and Avinash G. Keskar. "Copy Move Forgery Detection using DWT and SIFT Features." In Proceedings of 13th IEEE International Conference on Intelligent Systems Design and Applications (ISDA-2013), pp.188-193, December 2013.

[11] Anand, Vijay, Mohammad Farukh Hashmi, and Avinash G. Keskar. "A Copy Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods." In Proceedings of the 6th Asian Conference on Intelligent Information and

Licensed Under Creative Commons Attribution CC BY

Database Systems (ACIIDS 2014), Springer International Publishing, pp. 530-542, 2014.
[12] Bo, Xu, Wang Junwen, Liu Guangjie, and Dai Yuewei. "Image copymove forgery detection based on SURF." In Proceedings of IEEE International Conference on Multimedia Information Networking and Security (MINES-2010), pp. 889-892, 2010.
[13] Shivakumar, B. L., and S. SanthoshBaboo. "Detection of Region Duplication Forgery in Digital Images Using SURF." International Journal of Computer Science Issues (IJCSI), vol. 8, no. 4, pp.199-205, 2011.
[14] Mishra, Parul, Nishchol Mishra, Sanjeev Sharma, and Ravindra Patel. "Region Duplication Forgery Detection Technique Based on SURF and HAC." The Scientific World Journal, vol. 2013, Article ID 267691, pages 8, 2013.
[15] Al-Qershi, Osamah M., and Bee EeKhoo. "Passive detection of copymove forgery in digital images: State-of-the-art." Forensic Science International, vol. 231, no. 1, pp. 284-295, 2013.
[16] Li, Leida, Shushang Li, Hancheng Zhu, Shu-Chuan Chu, John F. Roddick, and Jeng-Shyang Pan. "An Efficient Scheme for DetectingCopy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp.46-56, January 2013.
[17] Lin, Liang, Xiaolong Wang, Wei Yang, and Jian-Huang Lai. "Discriminatively trained and-or graph models for object shape detection." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 37, no. 5 (2015): 959-972.
[18] Zoccolan, Davide. "Invariant visual object recognition and shape processing in rats." *Behavioural brain research* 285 (2015): 10-33.
[19] Cheng, Ming, Niloy J. Mitra, Xumin Huang, Philip HS Torr, and Song Hu. "Global contrast based salient region detection." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 37, no. 3 (2015): 569-582.
[20] Lei, Jie, Mingli Song, Ze-Nian Li, and Chun Chen. "Whole-body humanoid robot imitation with pose similarity evaluation." *Signal Processing* 108 (2015): 136-146.
[21] Zhang, Ruimao, Liang Lin, Rui Zhang, WangmengZuo, and Lei Zhang. "Bit-scalable deep hashing with regularized similarity learning for image retrieval and person re-identification." *Image Processing, IEEE Transactions on* 24, no. 12 (2015): 4766-4779.
[22] Quattoni, Ariadna, and Antonio Torralba. "Recognizing indoor scenes." In*Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on*, pp. 413-420. IEEE, 2009.
[23] Li, Li-Jia, Hao Su, Yongwhan Lim, and Li Fei-Fei. "Objects as attributes for scene classification." In *Trends and Topics in Computer Vision*, pp. 57-69. Springer Berlin Heidelberg, 2012.
[24] Antanas, Laura, Marco Hoffmann, Paolo Frasconi, Tinne Tuytelaars, and Luc De Raedt. "A relational kernel-based approach to scene classification." In*Applications of Computer Vision (WACV), 2013 IEEE Workshop on*, pp. 133-139. IEEE, 2013.
[25] Mesnil, Grégoire, Salah Rifai, Antoine Bordes, Xavier Glorot, Yoshua Bengio, and Pascal Vincent. "Unsupervised and Transfer Learning under Uncertainty-From Object Detections to Scene Categorization." In *ICPRAM*, pp. 345-354. 2013.
[26] Zhang, Lei, Xiantong Zhen, and Ling Shao. "Learning object-to-class kernels for scene classification." *Image Processing, IEEE Transactions on* 23, no. 8 (2014): 3241-3253.
[27] Li, Li-Jia, Hao Su, Li Fei-Fei, and Eric P. Xing. "Object bank: A high-level image representation for scene classification & semantic feature sparsification." In *Advances in neural information processing systems*, pp. 1378-1386. 2010.
[28] Alberti, Marina, John Folkesson, and Patric Jensfelt. "Relational approaches for joint object classification and scene similarity measurement in indoor environments." In *AAAI 2014 Spring Symposia: Qualitative Representations for Robots*. 2014.
[29] Russakovsky, Olga, Yuanqing Lin, Kai Yu, and Li Fei-Fei. "Object-centric spatial pooling for image classification." In *Computer Vision–ECCV 2012*, pp. 1-15. Springer Berlin Heidelberg, 2012.
[30] Espinace, Pablo, Thomas Kollar, Nicholas Roy, and Alvaro Soto. "Indoor scene recognition by a mobile robot through adaptive object detection." *Robotics and Autonomous Systems* 61, no. 9 (2013): 932-947.

Licensed Under Creative Commons Attribution CC BY