Digital Image Forensic based on Machine Learning approach for Forgery Detection and Localization

Monika¹ and Abhiruchi Passi²
¹Manav Rachna International Institute of Research & Studies, INDIA
²Manav Rachna International Institute of Research & Studies, INDIA

E-mail: monika.fet@mriu.edu.in, abhiruchi.fet@mriu.edu.in

Abstract. Machine learning for multimedia forensic is a new way of image forgery detection due to its amazing features of fast forgery detection. Compared with existing techniques of Deep Learning and Convolution Neural Network (“CNN”), machine learning improves security in the specific forged region under various test conditions. Some researchers use Support Vector Machine (“SVM”) and k-nearest neighbors (k-NN) algorithms to detect forgeries and another category uses unsupervised classification, including self-organization feature map (SOFM) and fuzzy c-means. But there occurs a need to address the detection speed improvement under the present scenario. The proposed algorithm has been developed using a machine learning approach to improve detection speed by pre-processing of feature extraction and feature reduction using “DWT” and “PCA” where data is trained by support vector machine (“SVM”) to provide quick results under various test conditions. This work specifies different image attacks like all types of geometric transformation, post-processing operations, etc., and presents efficiency in forgery detection and localization in case of multiple forgeries.

Index Terms—Machine Learning, Feature Extraction, Geometric Transformation, Multimedia Security, “SVM”.

1. Introduction
With the growth of Digital transformation, multimedia security and its originality is the major concern and issue for right message communication. Multimedia forensic is a new research area for providing authentic documents with the help of powerful machine learning tools and deep learning architecture. These tools provide more security-oriented applications as they are inherent to image attacks. In machine learning, many techniques are proposed for protecting learning systems including deep learning and neural network learning by focusing on image manipulation detection. The main focus is on secure machine learning-based forensics using the training and testing process. Forensic analysis is done via Support Vector Machine and some transformation is applied to achieve robust results for feature selection to train the classifiers. The next work is carried on method for forensic analysis as any processing performed on image leaves specific traces which helps to do forensic analysis by acquisition, coding, and processing. Deep Learning suffers from many limitations that restrict its application in the security of image forensic. Training of dataset is considered to give robust results by focusing on both support vector machine and Convolution Neural Network (“CNN”) classifiers. “CNN” is the programming model that helps the computer to learn from observational data. It is a class of deep neural networks that efficiently addresses various image processing tasks like pattern recognition but it is computationally a complex model as it is interconnected with large neurons. “CNN” features extraction is a data-driven process and has image classification as shape filters and a large dataset is required for the training and testing process. Figure 1 presents the simplest workflow consisting of hidden convolution parts for feature extraction and fully connected parts for classification. Machine learning
gives efficient performance but has drawbacks particularly in deep learning which suffers from security in terms of large data. Another limitation occurs during the test phase where output differs and there arises a need to generate a new class of machine learning forensic.

Figure 1. “Photo tampering throughout history.” “http://pth.izitru.com/ (Fake News)”

Figure 2. Categories of Machine Learning
According to Categories of Machine Learning, as described in Figure 2, in classification, inputs are divided into two or more classes, and the learner must produce a model that assigns unseen inputs to one or multi-label classification and can be handled by supervised learning. In regression, the supervised problem is generated where outputs are continuous rather than discrete. In Clustering, a set of inputs is to be divided into groups. Unlike in classification, the groups are not known beforehand, thus making this typically an unsupervised task. Density estimation finds the distribution of inputs in some space. Dimensionality reduction simplifies inputs by mapping them into a lower-dimensional space. Topic modeling is a related problem, where the program is given a list of human language documents and is tasked to find out which documents cover similar topics.

According to Classifier Evaluation Process, as described in Figure 3, the complete flow is presented where the choice of the learner is the major concern point to train the dataset for feature selections and further error measurements were tested through different strategies to evaluate classification. Figure 1 shows an example of image forgeries.

1.1 Basic machine Learning Concept

Machine learning is the learning distribution from input data. It is utilized to learn from experience E concerning some class of task T and performance measure P, if its performance at the task in T, as measured by P, improves with experience E. It is broadly divided into two classes that is supervised learning and unsupervised learning. Supervised learning is the latest research area and has practical applications like classification, Pattern recognition in computer vision, etc. It builds a model based on input data for which true class is known which is sampled from input data (Labeled data/Training data). It is also a data-driven process and the model will be only as good or as bad as the data we have. This means we cannot consider the data set of cap images and expect to use it to classify caps and rats. In this case, linear regression cannot be used to train a model on a dataset that does not have a linear correlation.

Machine learning under classification analysis task generates a statistical model with specific deficiencies like over-fitting and under-fitting. In the case of over-fitting, it occurs due to over-trained input data. This situation occurs as too many features are taken for input data and not enough data has been supplied. Another case is about under-fitting, and it occurs due to few features that are considered for training data thereby generating low and unreliable predictions. During training and testing, the learning procedure set of available data is divided into a training set for model training and a test set used for performance measuring. Under training, data validation is set to train the behavior concerning unseen data and then optimized for the choice of internal parameters of the algorithm.
1.2 “SVM”
Support Vector Machine (“SVM”) is the main tool of machine learning. “SVM” is designed for binary classification and multi-class classification. The advantages of “SVM”s include high accuracy. It works efficiently in practice and has been remarkably successful in such diverse fields as natural language categorization, bioinformatics, and computer vision. It also has tunable parameters and training optimization. It gives global and unique results by avoiding the convergence to local minima exhibited by other statistical learning systems, such as neural networks. The main aim is to find a hyperplane that has the maximum margin, i.e. a maximum distance between data from different classes which predicts that future data points will be correctly classified with high confidence. Feature extraction and feature reduction are extracted as parameters in the learning of the machine. The number of extracted features was reduced.

Figure 4. Classifier having limited attacks-sample strength in colored dots

2. Proposed Algorithmic Frame Work
Proposed work done in initial phase of image pre-processing and feature extraction with feature reduction process, performed efficiently to achieve the best feature to train the data set using “SVM”. Analysis is done through performance matrices which defines logical and mathematical designed construct to measure how close are the actual results from what has been expected or predicted. Error measurements are the main evaluation framework in this field. Initially, threshold segmentation is used for image segmentation based on a threshold value to turn a gray-scale image into a binary image and to simplify it in a more meaningful and easier analysis. Each of the pixels in a region is similar concerning some characteristics such as color, intensity, or texture. Adjacent regions are significantly different for the same characteristic. Feature Extraction analysis is done by Fourier transform which converts a time-domain signal into constituent sinusoids of different frequencies but is limited to discarding the time information of the signal. Thus, the quality of the classification decreases as time information is lost. Feature Reduction Excessive features increase computation time and storage memory. Furthermore, they sometimes make classification more complicated, which is called the curse of dimensionality. It is required to reduce the number of features. “PCA” is an efficient tool to reduce the dimension of a data set consisting of a large number of interrelated variables while retaining most of the variations. It is achieved by transforming the data set into a new set of ordered data according to their requirements. Table2(Kashyap et al., 2017) presents state-of-art and is further modified to current forgery detection status. Table1 shows the robustness of the proposed system and their results are presented in Figure8.
2.1 Proposed Scheme

![Workflow for the proposed forgery detection](image)

**Figure 5.** Workflow for the proposed forgery detection

3. Experiment Results

![Results show forgeries detected under various attacks](image)

**Figure 6.** Results show forgeries detected under various attacks
4. Result Analysis

Table 1. Run time comparative analysis of the proposed algorithm with existing methods

| Method                  | References                           | Time (s) |
|-------------------------|--------------------------------------|----------|
| Proposed Method         | Singh, G., & Singh, K. (2020). Elsevier | 25.00    |
| “DCT” & CFA             |                                      | 157.27   |

5. Conclusion

In recent years, researchers have proposed a lot of approaches for forgery detection, which falls into two categories where Supervised learning provides better results than unsupervised classifiers in terms of classification accuracy. Supervised classification methods used with “SVM”s are state-of-the-art classification methods based on machine learning theory. Compared with other methods such as artificial neural network, decision tree, and Bayesian network, “SVM”s have significant advantages of high accuracy as it does not need a large number of training samples to avoid over-fitting. This work presents the image forgery detection technique using a machine learning approach to improve detection speed by pre-processing of feature extraction and feature reduction using “DWT” and “PCA” where data is trained by support vector machine (“SVM”) to provide results in 25 seconds.

Acknowledgment

Thanks to the reviewers to share valuable comments to improve the quality.

Table 2. Review the state-of-the-art in CMFD Methods.

| S.N. | “Paper title”                                      | “Method”                                                   | “Type of Forgery”                      | “Outcomes”                                                   | Year |
|------|----------------------------------------------------|------------------------------------------------------------|----------------------------------------|--------------------------------------------------------------|------|
| 1.   | “Image forensic approach based on the second-order statistical analysis of CFA artifacts” | MTTPM, Re-Interpolation, CFA artifacts | Detection Speed is limited | 2020 |
| 2.   | “Investigation of image forgery based on multi-scale under illumination variations” | “Statistical region merging (SRM), multiscale census transform (MI-CSCT) descriptor & fuzzy C means (FCM)” | Forgery detection under different illumination changes | “Fine features are extracted based on multiscale (MSR) with color distribution” | 2020 |
| 3.   | “An efficient method for image forgery detection based on trigonometric transforms and deep learning” | “Convolutional Neural Network (“CNN”), Deep learning, Trigonometric transforms” | Detect and extract features for active and passive forgery detection | “Accuracy with deep learning reached 100%” | 2020 |
| 4.   | “Forensic Similarity for Digital Images” | Deep-learning system (“CNN”-based feature extractor)and neural network | Forensic similarity | Significantly improves efficacy on “unknown” forensic traces | 2020 |
| 5.   | “A novel image retrieval method based on multi-features fusion” | Weighted adjacent structure. Captured fusion features of an image. | Superior performance in content-based image retrieval. | 2020 |
| 6.   | “A PUF-Based Data-Device Hash for Tampered Image” | Physical unclonable function (PUF) | TSMS technology | “Tamper detection rate of 95.42% authentication performance of above 98.5%” | 2020 |
| No. | Approach                                                                 | Technique/Algorithm                                                                 | Results/Remarks                                                                 | Year |
|-----|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|------|
| 7   | Detection and Source Camera Identification                                | “Fusing Cross-modal semantic translation, Supervised learning-based methods”        | “Automatically translate image-level text semantic labels into several pixel-level image regions” | 2020 |
| 8   | Image understanding via Learning Weakly-supervised Cross-modal Semantic Translation | “Automatic threshold selection based on iterative means of regions size as the filtering process.” | “Copy-move forgery (CMF) detection methods against image quality, sizes and attacks” | 2020 |
| 9   | An Embedding Strategy on Fusing Multiple Image Features for Data Hiding in Multiple Images | Gray level co-occurrence matrix for Stefano graphical algorithms                    | Fusing multiple features detected                                               | 2020 |
| 10  | “CMF-iteMS: An automatic threshold selection for detection of copy-move forgery” | “Copy-move region detected”                                                         | “Higher security performance against the blind universal pooled steganalysis”   | 2020 |
| 11  | An improved median filtering anti-forensics with better image quality and forensic undetect ability | “Total Variation -based minimization -Image variational deconvolution”               | Superior results in terms of image visual quality                               | 2020 |
| 12  | An End-to-End Dense-Inception Net for Image Copy-Move Forgery Detection | “Multi-dimensional dense-feature connection, Deep Neural Network (DNN)”               | “Best performance against most known attacks.”                                  | 2019 |
| 13  | Gradient-Based Illumination Description for Image Forgery Detection      | physics-based methods, lighting direction, image gradient,                          | Copy-move region detected                                                       | 2019 |
| 14  | Detection of splicing forgery using wavelet decomposition                | wavelet decomposition                                                               | Splicing type of forgery detected                                               | 2015 |
| 15  | Video frame copy-move forgery detection based on cellular automata and local binary patterns | “Cellular automata and local binary patterns”                                       | “Copy-move region detected”                                                     | 2014 |
| 16  | Speeding-up SIFT based copy-move forgery Detection using level set approach | “SIFT”                                                                             | “Copy move region is detected”                                                   | 2014 |
| 17  | “Shape-based copy-move forgery detection using level set approach”      | “Level set approach”                                                               | “Copy-move region detected”                                                     | 2014 |
| 18  | “Jpeg copy-paste forgery detection using bag Optimized for complex images” | “Bag Optimized for complex images”                                                 | “Forged region is detected”                                                      | 2014 |
| 19  | “Copy-rotation-move forgery detection using the Mrogh descriptor”       | “Copy move region detected”                                                        | “Highly efficient”                                                              | 2014 |
| No.  | Title                                                                                                                | Methodology                                                                 | Results                                                                 | Year   |
|------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|--------|
| 20.  | “Copy-rotate-move forgery detection based on Spatial domain”                                                        | “Spatial domain”                                                           | “Forged region is detected”                                            | 2014   |
| 21.  | “Copy-move image forgery detection Based on SIFT descriptors and SVD-matching”                                       | “SIFT descriptors And SVD-matching”                                         | “Forged region is detected”                                            | 2014   |
| 22.  | “Copy-move forgery detection based on patch match”                                                                      | “Patch match, an iterative Randomized algorithm for the nearest-neighbor search” | “Copy-move region detected”                                            | 2014   |
| 23.  | “Adaptive Matching For CopyMove Forgery Detection”                                                                     | “Block-Based Method using Adaptive Threshold.”                               | “Copy-Move Region Is Detected”                                          | 2014   |
| 24.  | “A scheme for copy-move forgery detection in digital images based on 2D-DWT”                                         | “2D-DWT”                                                                   | “Copy-move region is detected”                                          | 2014   |
| 25.  | “A copy-move image forgery detection based on Speeded up robust feature transform and wavelet Transforms”            | “Speeded up robust feature transform and wavelet Transforms”                | “Forged region is detected accurately.”                                 | 2014   |
| 26.  | “Video copy-move forgery detection and Localization based on Tamura texture features”                               | “Tamura texture features”                                                  | “Copy-move region detected”                                            | 2013   |
| 27.  | “Detection of copy-move forgery using krawtchouk moment”                                                              | “Krawtchouk moment”                                                        | “Copy-move region detected”                                            | 2013   |
| 28.  | “Detection of copy-move forgery using wavelet Decomposition”                                                          | “wavelet Decomposition”                                                    | “Copy-move region detected”                                            | 2013   |
| 29.  | “Copy-move image forgery detection using local binary pattern and Neighborhood clustering”                             | “Local binary pattern and Neighborhood clustering”                           | “Copy-move region detected”                                            | 2013   |
| 30.  | “Copy-move forgery detection in images via 2D-Fourier transform”                                                     | “2D- Fourier transform”                                                     | “Copy-move region detected accurately.”                                 | 2013   |
| 31.  | “Copy move image forgery detection using mutual Information”                                                          | “Mutual information”                                                       | “Copy-move region detected”                                            | 2013   |
| 32.  | “Copy move image forgery detection method using Steerable pyramid transform and texture descriptor”                  | “Steerable pyramid transform local binary pattern (LBP), and texture descriptor” | “Copy move region is detected”                                         | 2013   |
| 33.  | “Copy move forgery detection using DWT and SIFT features”                                                             | “DWT” and “SIFT”                                                            | “Copy move region is detected”                                         | 2013   |
| 34.  | “A fast “DCT” based method for copymoveforgeryDetection”                                                              | “DCT”                                                                      | “Copy-move region is detected”                                          | 2013   |
| No.  | Title                                                                 | Method                                                                 | Description                                                                 | Year |
|------|-----------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------|------|
| 35   | “A robust image copy-move forgery detection Based on mixed moments”    | “Mixed moment, gaussian pyramid transform”                              | “Tampered region is precisely detected”                                    | 2013 |
| 36   | “Detection of copy-move forgery in digital images Using radon transformation and phase correlation” | “Radon transformation and phase correlation”                             | “Exact copy-move region is detected”                                       | 2012 |
| 37   | “Detection Of Copy-Move Forgery Image Using Gabor Descriptor”          | “Gabor Descriptor”                                                     | “Copy Move Region Detected”                                                | 2012 |
| 38   | “Copy-move image forgery detection using multi-resolution weber Descriptors” | “Multi-resolution weber Descriptors”                                   | “Copy move region detected”                                                | 2012 |
| 39   | “Copy-Move Forgery Detection In Digital Images Based On Local Dimension Estimation” | “Local Dimension Estimation”                                           | “Copy-Move Region Detected”                                                | 2012 |
| 40   | “Copy-move forgery detection based on PHT”                             | “Polar harmonic transform(PHT)”                                        | “Scheme can detect the copy-move forgery When the copied region is rotated before being pasted.” | 2012 |
| 41   | “An evaluation of popular copy-move forgery detection approaches”      | “DCT”, “DWT”, “K”, “PCA”, “PCA”                                       | “Copy move region detected”                                                | 2012 |
| 42   | “A fast image copy-move forgery detection method using phase correlation” | “Phase correlation”                                                   | “Copy move region detected”                                                | 2012 |
| 43   | “Image copy-move forgery detection based on crossing shadow division”  | “DWT” and crossing shadow                                              | “Copy-move region detected”                                                | 2011 |
| 44   | “Detection of copy-create image forgery using Luminance level techniques” | “Luminance level techniques”                                           | “Copy-create image forgery”                                                | 2011 |
| 45   | “Detecting copy-paste forgeries using transform-invariant features”    | “Transform-invariant features”                                         | “Copy-paste forgery detection”                                             | 2011 |
| 46   | “Detecting copy-move forgery using non-negative matrix factorization” | “Non-negative matrix factorization”                                    | “Copy-move region is detected”                                             | 2011 |
| 47. | “Copy-move forgery detection using dyadic wavelet transform” | “Dyadic wavelet transform” | “Imagesegmentation and similarity detection” | “Not efficient for complicated background and texture” | 2011 |
| 48. | “Blind copy-move image forgery detection Using dyadic undecimated wavelet transform” | “Dyadic undecimated wavelet transform” | “Copy-move region is detected” | “Will not work in the noisy image” | 2011 |
| 49. | “Copy-move forgery detection in the digital image” | “SVD” | “Forged region is detected” | “Will not work well in the noisy image” | 2010 |
| 50. | “Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis” | “Double Quantization DCT” | “Tampered region is detected accurately” | “Works only in JPEG Format” | 2009 |
| 51. | “Detect digital image splicing with visual cues” | “DW-VAM” | “In the spliced image, the forged region is detected” | “Work only in the Splicing” | 2009 |
| 52. | “Fast copy-move forgery detection” | Improved “PCA” | “Exact Copy-Move region is detected” | “Works well in the noisy, compressed image” | 2009 |
| 53. | “Identifying tampered regions using singular value decomposition in Digital image forensics” | “SVD” | “Copy-Move region is detected accurately” | “Will not work in highly noised and compressed image” | 2008 |
| 54. | “Detection of copy-move forgery in digital images using the SIFT algorithm” | “SIFT” | “Copy-move region is detected” | “Detects false result also” | 2008 |
| 55. | “A new approach for detecting copy-move forgery detection in the digital image” | “DWT” | “Exact copy-move region is detected” | “Works well in the noisy and compressed image” | 2008 |
| 56. | “A sorted neighborhood approach for detecting duplicate reason based on DWT and SVD” | “DWT” and “SVD” | “DWT-SVD Efficiently detects forged region” | “Time complexity is less compared to other algorithms” | 2007 |
| 57. | “Robust detection of region duplication in the digital image” | “Similarity matching” | “Copy-move region detected in noisy conditions” | “Time complexity is reduced” | 2006 |
| 58. | “Exposing digital forgeries by detecting duplicated image regions” | “PCA” | “Exact copy-move region is detected automatically” | “Time complexity is high” | 2004 |
| 59. | “Detection of copy-move forgery in the digital image” | “DCT” | “Copy-move region is detected” | “Will not work in the noisy image” | 2003 |

**References**

[1] Cozzolino, D., & Verdoliva, L. (2020). Noiseprint: A CNN-Based Camera Model Fingerprint. *IEEE Transactions on Information Forensics and Security, 15*(1), 144–159.

[2] Al_Azrak, F. M., Sedik, A., Dessowky, M. I., El Banby, G. M., Khalaf, A. A. M., Elkorany, A. S., & Fathi, F. E. (2020). An efficient method for image forgery detection based on trigonometric transforms and deep learning. *Multimedia Tools and Applications, 79*(25–26), 18221–18243.

[3] Mayer, O., & Stamm, M. C. (2020). Forensic Similarity for Digital Images. *IEEE Transactions on Information Forensics and Security, 15*(1), 1331–1346.

[4] Matern, F., Riess, C., & Staminger, M. (2020). Gradient-Based Illumination Description for Image Forgery Detection. *IEEE Transactions on Information Forensics and Security, 15*(c), 1303–1317.

[5] Niu, D., Zhao, X., Lin, X., & Zhang, C. (2020). A novel image retrieval method based on multi-features fusion. *Signal Processing: Image Communication*.

[6] Zheng, Y., Cao, Y., & Chang, C. H. (2020). A PUF-Based Data-Device Hash for Tampered Image Detection and Source Camera Identification. *IEEE Transactions on Information Forensics and Security, 15*(X), 620–634.
[7] Singh, G., & Singh, K. (2020). Image forensic approach based on the second-order statistical analysis of CFA artifacts. Forensic Science International: Digital Investigation, 32, 200899.

[8] Shen, G. (2020). Image Understanding via Learning Weakly-supervised Cross-modal Semantic Translation. Journal of Visual Communication and Image Representation, 102789.

[9] Junxue Yang, X. L. (2020). An Embedding Strategy on Fusing Multiple Image Features for Data Hiding in Multiple Images. Journal of Visual Communication and Image Representation, 102822.

[10] Nor, N. B., Idris, M. Y. I., Abdul Wahab, A. W., Salleh, R., & Ismail, A. (2019). CMF-iteMS: An automatic threshold selection for detection of copy-move forgery. Forensic Science International, 295, 83–99.

[11] Singh, K., Kansal, A., & Singh, G. (2019). An improved median filtering anti-forensics with better image quality and forensic undetectability. Multidimensional Systems and Signal Processing, 30(4), 1951–1974.

[12] Zhong, J.-L., & Pun, C.-M. (2019). An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection. IEEE Transactions on Information Forensics and Security, 15(c), 2134–2146.

[13] Malathi, J., Narasimha Swamy, B., & Musunuri, R. (2019). Image forgery detection by using machine learning. International Journal of Innovative Technology and Exploring Engineering, 8(6 Special Issue 4), 561–563.

[14] Barad, Z. J., & Goswami, M. M. (2020). Image Forgery Detection using Deep Learning: A Survey. 2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS 2020, 571–576.

[15] Butora, J., & Fridrich, J. (2020). Reverse JPEG Compatibility Attack. IEEE Transactions on Information Forensics and Security, 15(c), 1444–1454.

[16] Fadl, S. M., Han, Q., & Li, Q. (2019). Inter-frame forgery detection based on differential energy of residue. IET Image Processing, 522–528.

[17] Darvish, M., Hosseini, M., & Kirchner, M. (2019). Unsupervised Image Manipulation Localization With Non-Binary Label Attribution. IEEE Signal Processing Letters, PP(c), 1.

[18] Teerakanok, S., & Uehara, T. (2019). Copy-move Forgery Detection: A State-of-the-Art Technical Review and Analysis. IEEE Access, (c), 1.

[19] Głowb, P., Romaszewski, M., Cholewa, M., & Domino, K. (2018). Application of hyperspectral imaging and machine learning methods for the detection of gunshot residue patterns. Forensic Science International, 290, 227–237.

[20] Kashyap, A., Parmar, R. S., Agarwal, M., & Gupta, H. (2017). An Evaluation of Digital Image Forgery Detection Approaches. Cs.MM.