Deep Learning based Counter–Forensic Image Classification for Camera Model Identification

Venkata Udaya Sameer, Ruchira Naskar, Nikhita Musthyala, and Kalyan Kokkalla

Department of Computer Science and Engineering,
National Institute of Technology, Rourkela
Odisha, India–769008.
{515CS1003,naskarr,714cs2045,114cs0359}@nitrkl.ac.in

Abstract. *Camera Model Identification* is the digital forensic problem of identifying the source of an image under question, i.e., to map the image to its source device. This assists forensic analysts to map a suspect's camera with a possibly illegal image repository, or to attribute an image under question to its legitimate source. Counter–forensic attacks to Camera Model Identification techniques, primarily comprise of image anonymization. *Image Anonymization* is a technique adopted by an intelligent adversary for modifying an image illegitimately, so as to disable attribution of the image to its source; hence to fool a forensic analyst and prevent image source identification. In the recent years, there has been a rapid growth of research interest in the domain of counter–forensics. In this paper, we develop a deep learning based Convolutional Neural Network (CNN) to detect whether an image under question has undergone any form of counter–forensic source anonymization attack. This will enable a forensic analyst to find out whether an image, whose source is being investigated, is authentic, or has it been tampered so as to prevent correct source identification. We deal with three major classes of source anonymization attacks in this paper, viz., *Seam Carving*, *Fingerprint Copying*, and *Adaptive PRNU Denoising*. If an image is detected to have indeed undergone a counter–forensic attack, the proposed model additionally enables detection of the specific class of attack, through multiclass classification. Our experimental results prove that the detection accuracy of the proposed system is considerably high, and it passes the overfitting test too.

Keywords. Classification, Convolutional Neural Network, Counter–Forensics, Deep Learning, Digital Forensics, Source Camera Identification.

1 Introduction

Digital Forensics is a branch of science which helps law enforcement agencies in providing legal evidences to digital crimes. In today's digital era, digital crime rate is on a high rise. *Digital image forensics* [1] is a sub–area of digital forensics that deals with images involved in the digital crime scenarios. *Camera Model Identification* [2–13], is the problem of identifying the legitimate source of an

image under question, through forensic investigations. This is primarily done by attributing an image to its source using camera fingerprints such as Photo Response Non Uniformity (PRNU) or through a machine learning classification using feature such as Image Quality Metrics (IQM), High Order Wavelet Statistics (HOWS) etc.

Counter–forensics with respect to camera model identification [14, 15, 17, 16, 18] are aimed towards defeating state–of–the–art camera model identification techniques by fooling the forensic analysis process. Counter–forensic attacks against camera model identification are majorly comprised of *source anonymization* techniques. *Source anonymization* is a form of intelligent adversarial attack, which hinders source attribution of images through illegitimate image modifications. Such attacks are motivated by image anonymization works [14] that aim at user anonymity, which are of relevance in protecting the privacy of on–line users. However, image anonymity acts as a hindrance to forensic image source identification.

Recent counter–forensic techniques [14, 15, 17, 16, 18] have proved to be quite effective in battling state–of–the–art camera model identification. Hence, it is imperative that the state–of–the–art camera model identification techniques be made capable enough to resist counter–forensic attacks. In this context, here we propose a deep learning based classification model using Convolutional Neural Networks (CNN) to detect whether an image (to be analyzed forensically) is authentic, or it has undergone counter–forensic modifications which would result in invalidation of the forensic analysis results.

Our major contribution in this paper is the development of a deep learning based CNN model for classification between authentic and counter–forensically modified images. In addition, the proposed model performs a second level of (multi–class) classification to identify the specific class of counter–forensic attack the (tampered) image has undergone. The performance of a machine learning system largely depends on how effectively features of the concerned dataset are identified and extracted. Many artificial intelligence problems are solved through machine learning, only when the appropriate features are successfully identified and extracted. It is this dependency of machine learning based models on the representation (features) of the data, that many times makes such systems ineffective; specifically, when the features are difficult to be identified. *Deep Learning* is a fast emerging trend, where feature identification and extraction is taken care of by the underlying neural network, i.e., the deep learning network does a representation learning for the given data. We utilize this ability of a deep neural network to perform a representation learning of counter–forensic images and hence to develop a classification model for those. A *Convolutional Neural Network* (CNN), used to build the proposed model in this work, is a special type of deep neural network which is based on linear mathematical convolution.

In Fig. 1, we present the operational flowchart of the proposed two–level classification system. Fig. 1 shows that proposed model primarily consists of a *counter–forensic detection module*, which is a deep learning network (CNN), that detects whether the image is authentic or counter–forensically modified. If

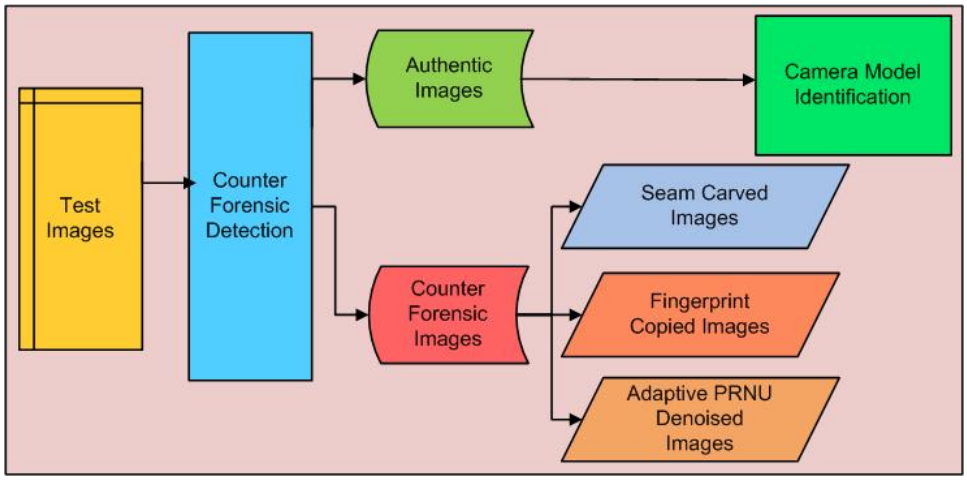

Fig. 1. Operational flowchart of the proposed model for classification of counter–forensic images with respect to camera model identification.

an image is detected to be authentic, it is taken up for forensic investigations. Else, if the image is detected to be counter–forensically modified, the proposed model tries to identify the class of source anonymization performed on it, so as to assist the forensic analyst to adopt possible measures for retrieving the image back to its original form. This is done by a multi–class classification among the major classes of state–of–the–art source anonymization techniques, using deep learning.

In this paper, we deal with the three broad classes constituting the state–of–the–art in source anonymization, viz., *Seam Carving* [14, 15], *Fingerprint Copying* [16], and *Adaptive PRNU Denoising* [17]. Our experimental results prove that the classification accuracy of the proposed model is considerably high.

The rest of the paper is organized as follows. In Section 2, we present the relevant background on camera model identification and related source anonymization techniques. In Section 3, we present the proposed deep learning Convolutional Neural Network model for classification of source anonymized images. Our experimental results are presented in Section 4. Finally, we conclude with future research directions in Section 5.

2 Background

In the existing state–of–the–art, there are mainly two approaches to image source identification, viz., fingerprint based approach [5, 7, 19] and feature based machine learning approach [2–4, 8–11, 21]. We discuss the basic operation of both the approaches in Section 2.1. In Section 2.2 we present relevant background on existing counter–forensic (source anonymization) attacks on camera model identification.

2.1 Camera Model Identification

Kharrazi et al. [2] proposed a feature based image source iedntification technique, by representing an image as a set of numerical features. The features are computed in both spatial domain (Image Quality Metrics (IQM)) and wavelet domain (High Order Wavelet Statistics (HOWS)). Ever since, several researchers have used different image feature sets to perform camera model identification. Those include Binary Similarity Metrics (BSM) used by Celiktutan et al. [3], features based on Color Filter Array (CFA) interpolation used by Bayram et al. [4], extended color feature set used by Gloe et al. [21], image texture features like Local Binary Pattern (LBP) and Local Phase Quantization (LPQ) features used by Bing et al. [9], ensemble of demosaicing features used by Chen et al. [11], among others. Supervised machine learning based classification techniques (such as Support Vector Machine (SVM)) are used in the above researches to perform classification among different camera models.

In fingerprint based techniques for image source identification, Photo Response Non–Uniformity (PRNU) noise has been used as unique camera fingerprint to map an image to its source [5, 7, 19]. PRNU of a test image, and Sensor Pattern Noises (SPN) of possible camera models are computed, and a correlation mechanism between those is employed to correlate an image to its source. Correlation mechanisms used in the literature include Normalised Cross Correlation (NCC) [5] and Peak to Correlation Energy (PCE) [6].

Very recently, a number of researchers have started using deep learning techniques in camera model identification [12, 13]. In these works, different deep learning architectures are studied and the deep neural networks are tuned to perform efficient camera model identification. In [12] a simple CNN is trained for camera model identification and in [13], a CNN followed by a transfer learning using SVM is proposed. Both these techniques offer a new perspective to camera model identification as there is no pre–processing step involved. In case of a feature based techniques, the pre–processing involved consists of feature engineering; and in case of fingerprint based techniques, sensor patter noise and PRNU computations.

2.2 Counter–Forensics for Image Source Identification

As stated previously, image source anonymization is the major form of counter–forensic attack against camera model identification. Next, we discuss the basic operating principles of the three major classes of source anonymization algorithms, viz., *Seam Carving* [14, 15], *Fingerprint Copying* [16], and *Adaptive PRNU Denoising* [17].

Seam Carving *Seam Carving* [22] is a content aware resizing approach which finds wide use in counter–forensics [14, 15]. Seam carving technique is used to disturb an image's reference noise pattern, so as to defeat PRNU based image source attribution, which operates by correlating image noise pattern with (possible) camera reference patterns.

Specifically, seam carving disturbs the PRNU content of an image through image resizing, thus removes *seams* (connected paths of pixels with least variation from surrounding pixels) [22] of an image. For an image with m rows and n columns, a vertical seam s is nothing but a path connecting pixels from top to bottom with horizontal offsets (between adjacent rows) not more than one pixel, and is represented mathematically as,

$$s = \{s_i\}_{i=1}^{n-1} = \{(col(i), i)\}_{i=1}^{n-1}, \text{ where } |col(i+1) - col(i)| \leq 1 \tag{1}$$

where i represents an image column and $col(i)$ is a mapping from $[1 \cdots n]$ to $[1 \cdots m]$. The seam is a 8–connected path from top to bottom, with exactly one pixel per row. Finally, the pixels forming the seam s would be $I(s_i)_{i=1}^{n-1} = I(col(i), i)_{i=1}^{n-1}$.

An optimal seam (s^*) is the seam with the lowest sum of energy [22], where the energy function is given by,

$$e(I) = \left|\frac{\partial I}{\partial x}\right| + \left|\frac{\partial I}{\partial y}\right| \tag{2}$$

and, an optimal seam (s^*) is computed as,

$$s^* = \min_s \sum_{i=1}^{n} e(I(s_i)) \tag{3}$$

It is evident from the above equation that the optimal seam is computed using the cumulative minimum energy, for all possible connected seams, from the first to the last column. Such optimal seams are removed from the original image to get a seam carved image.

What makes a seam carved image difficult to analyse, is the lack of information about the location or number of its seams removed. This is because the process of seam carving is irreversible, and the PRNU pattern of the seam carved image, will correlate very poorly with noise reference pattern of its source.

Fingerprint Copy Attack *Fingerprint copy* [16, 23], as the name suggests, is the technique of masking one camera reference pattern with another. The adversary masks his own camera pattern with another innocent's camera pattern, thus resulting into high rate of false positives in camera model identification. In a sensitive forensic application as camera model identification, it is of paramount importance to keep the false positive alarms minimal. Hence, the fingerprint copy attack poses as an imminent threat to the credibility of the forensic source identification systems, by leading an innocent to be detected wrongly as culprit.

Fingerprint copy attack is delivered as follows. Let image I be originating from camera A, possessed by an adversary. Let us assume that the adversary additionally gets access to some images captured by some other person's camera B, and estimates the noise residuals of both cameras A and B, NR_A and NR_B

respectively, from the available images. Now, he removes his camera's fingerprint from I, and adds the fingerprint of B to I, by the following:

$$\tilde{I} = I - \alpha \times NR_A + \beta \times NR_B \tag{4}$$

where NR_A and NR_B are the noise residuals of cameras A and B respectively, and α and β are the camera substitution parameters that determine the strength of the fingerprint copy.

As a result, the forensic analyst is fooled to believe that image I originated from camera B, and not from A, as a result of his investigations. This renders the owner of camera B to be the culprit, instead of that of camera A.

Adaptive PRNU Denoising (APD) Image PRNU is resilient to various geometric and compression manipulations [5]. Hence to make an image untraceable to its source camera, different attacks started targeting the PRNU content of an image, a major identifier of the underlying sensor. *Adaptive PRNU Denoising* (APD) [17] is one such counter–forensic attack which denoises an image, repetitively, until it has sufficiently suppressed the image PRNU to prevent its source identification. In the following Eq. 5, a Denoising Filter (DF) is applied m times to suppress the noise residual of an image I.

$$\hat{I} = DF(DF(DF \cdots m\ times\ (I))) = DF^m(I) \tag{5}$$

The objective is to obtain an image which would correlate very poorly with its own PRNU noise pattern. In order to achieve this, the PRNU estimate of the image I (NR_I) is computed as in [5], and a magnitude adjustment factor β is estimated according to Eq. 6 below.

$$Corr((I - \beta \times NR_I), NR_I) \approx 0 \tag{6}$$

APD lowers the correlation of an image to its source efficiently, without affecting any visual artifact. Since no additional artifacts are introduced due to repeated denoising, to detect whether an image has undergone this process, is difficult.

The existing counter–forensic techniques presented above, are extremely efficient in defeating state–of–the–art camera model identification methods. Hence it would be helpful to distinguish between authentic and counter–forensic images, so as not to fool the forensic investigations. As of yet no suitable feature or common artifacts have been identified, which are capable enough to distinguish counter–forensic images. Hence we adopt a deep learning architecture in this work, for the task of counter–forensic image classification, whereby the feature learning happens through deep neural network.

3 Proposed Deep Learning based Convolutional Neural Network (CNN) Model for Counter–Forensic Image Classification

In a machine learning based classification system, the feature representations have to be accurately defined. However, in scenarios where it is impossible or difficult to pre–define a feature representation of given dataset, machine learning techniques are bound to fail. Deep learning techniques, having the ability to acquire knowledge through the inherent characteristics of training data where the knowledge acquired is stored as the weights of the network, overcomes this limitation of machine learning models. Regular neural networks do perform well in image classification, but due to high computational complexity and as the weights in successive layers keep on increasing, having a full connectivity in every layer, would involve huge number of parameters, and quickly lead to overfitting. Convolutional Neural Networks (CNN) [27] constitute a type of deep learning neural networks, which perform well with images. They have been found to be useful in various computer vision and image processing applications, such as object recognition [26], number recognition from hand written text etc. [27].

In this paper, we use convolutional neural networks to perform a two stage classification for counter–forensic images. First, a binary classification to separate counter–forensic images from authentic ones, and second, a multi–class classification to identify the type of counter–forensic image. The proposed CNN architecture is shown as a block diagram in Fig. 2, which includes the followings:

- The first convolution layer (Conv1) with a 3×3 kernel and 32 filters, followed by a Rectifier Linera Unit (ReLU).
- The second convolution layer (Conv2) with a 3×3 kernel and 32 filters, followed by another ReLU.
- Max Pooling with a 2×2 window, followed by the first dropout layer (DropOut1) with drop out parameter 0.2.
- A fully connected layer, followed by a ReLU activation, which is subsequently followed by the second dropout layer (DropOut2) with drop out parameter of 0.5.
- A fully connected layer, followed by a softmax layer for loss computation.

Next, we describe in detail, the structure of different layers (specified above) used in this architecture, along with the importance of each.

3.1 Convolution

The major operation performed in a CNN is *convolution*. Convolutional networks are simply neural networks, that use convolution in place of general matrix multiplication in at least one of their layers [24]. The convolution operation [25] on a signal S, using a window W, is defined as follows:

$$C(t) = \int S(x)W(t-x)dx \tag{7}$$

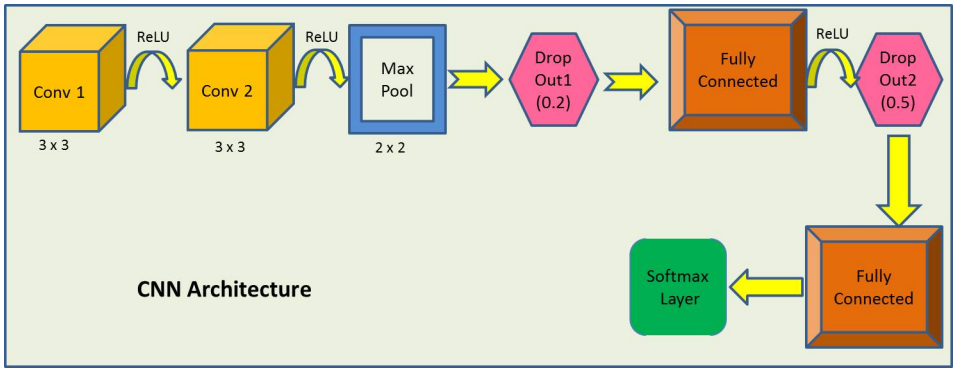

Fig. 2. Proposed CNN architecture for counter–forensic image classification.

In CNN terminology, the first argument to a convolution operation ($S(x)$ in Eq. 7) is called the *input* and the second argument ($W(t-x)$ in Eq. 7) is called the *kernel*. The output of the convolution operation is a *feature map* ($C(t)$ in Eq. 7).

On a two dimensional signal, such as an image I, of dimension $m \times n$, using a kernel K, the convolution operation is carried out as follows:

$$C(i,j) = \sum_m \sum_n I(m,n)K(i-m, j-n) \tag{8}$$

From each test image I (authentic or counter–forensic), we crop out a central portion (of size 32×32, 64×64 or 128×128), which are fed as input to the proposed CNN in batches of sizes 64, 128 and 256. Here, we use two convolution layers with 32 filters and kernel of size 3×3 each. In the next section, we describe the activation and pooling types used in this work.

3.2 Activation and Pooling

A CNN performs three primitive operational steps while doing a classification. It starts with a convolution operation using a specific kernel, then uses an activation function in the *detector stage* for feature extraction, and finally enhances the output further, through a *pooling* layer. An activation function takes the output of the previous layer which is nothing but a weighted data and produces a non–linear transformation of the data. Most used activation functions include sigmoid ($\frac{1}{1+e^{-x}}$) and tanh ($f(x) = tanh(x)$), (x being the input signal) [24]. Rectified Linear Units (ReLU) are used extensively in deep learning to achieve *non–linearity*. In a ReLU, $f(x) \approx log(1+e^x)$, where x is the input signal.

In this paper, we use three ReLU activations to introduce non–linearity in the layers. The advantage of a ReLU over a Sigmoid function is that the gradient of sigmoid function reaches approximately zero when we increase or decrease x; but in case of a ReLU, the gradient does not vanish when x is varied.

In the pooling layer, the output of the previous layer at a particular position is replaced with the summary statistics of its neighborhood. The popular pooling mechanisms adopted are, max pooling (which replaces the value with the maximum element in the pre–defined neighborhood), average pooling (which replaces the average value of the pre–defined neighborhood), L^2 norm of neighborhood (which replaces the value with square root of sum of squares of the activations in the neighborhood). In this paper, we use a max pooling layer with a 2×2 window. Next, we describe the type of optimizer used in our CNN.

3.3 Optimizer

The most important module involved in a neural network is the performance evaluation of the learning task at hand, to measure how well the network is able to optimize the cost function $J(\theta)$ (where θ is the parameter space of the architecture). The cost function in this paper is considered to be the 'classification error'. Hence, in this work, the objective is to minimize the classification error, i.e., to minimize the cost function.

The function of the *optimizer* in a CNN is to find the optimal set of θ values, i.e., the set which would optimize cost function $J(\theta)$. The types of optimizers used commonly in deep learning are, *Stochastic Gradient Descent, RMS Prop, Adam, AdaDelta [24]* etc.

In this paper, we use Stochastic Gradient Descent optimizer, with a learning rate of 0.01, and momentum fixed at 0.9. Additionally, dropout layers are used in the proposed CNN to overcome overfitting. In a dropout layer, the updation of weights of random nodes is stopped, so that the network is forced to learn independent representations of the data, and hence to prevent overfitting.

4 Experimental Results

In this section we provide our experimental results to measure the accuracy of the proposed deep learning model in classifying counter–forensic images.

4.1 Experimental Setup

We conducted our experiments on the Dresden Image Database [20], which is a benchmark dataset, available publicly for image forensic research. In this work, we have used a total of 12,500 natural images of the Dresden database, for our experiments, out of which 5,000 are authentic and the rest 7,500 are counter–forensically modified. The 7,500 counter–forensic images, consist of three sets of 2,500 images, modified manually through seam carving, fingerprint copy attack and Adaptive PRNU Denoising, respectively, following the procedure discussed in Section 2.2.

The proposed CNN takes input on varied batches as 64, 128 and 256 for 32×32, 64×64 and 128×128 image blocks. The proposed network architecture is presented in Fig. 2. A 3×3 kernel is used in convolution and a 2×2 window

in max pooling layer. The convolution layers are followed by a ReLU activation to introduce non–linearity. All the different batches are trained using Stochastic Gradient Descent (SGD) with a momentum fixed at 0.9, learning rate of 0.01 and decay of 0.005. Two drop–out layers are used to fight overfitting with dropout probabilities 0.2 and 0.5 respectively. The last layer is a softmax layer that computes the loss function.

In our work, the CNN training is carried out using the keras [28] framework developed for deep learning. We have used a workstation with an Intel Xeon CPU (E3-1225 v5, 3.3GHz), 16GB RAM and a GPU (Geforce GTX 970) with 1664 CUDA cores.

4.2 Performance of the Proposed Model

Experiment 1 The first step in our proposed methodology is to perform a binary classification between authentic and counter–forensic images. The training samples are labelled with two classes: authentic (5000 samples) or counter–forensic (7500 samples). The confusion matrix representing the binary classification results, is shown in Table 1. The overall classification accuracy achieved is 93.4%.

Experiment 2 In the second step, the counter–forensic images are further classified according to the class of source anonymization attack that they have undergone (seam carved, fingerprint copied, or APD). We used 2500 labelled training samples from each type of counter–forensic class. In Table 2, we present the second level classification accuracy results between seam carved, fingerprint copied, and PRNU denoised images, with varied image sizes (32×32, 64×64 and 128×128) and batch sizes $(64, 128, 256)$.

In our experiments, we achieve the maximum classification accuracy of 85.7% for image size 64×64, and batch size 128, using a stochastic gradient descent optimizer with learning rate of 0.01 and momentum of 0.9.

As evident from Table 2, the classification accuracy varies with image (crop–out) size. We observe the the best performance with 64×64 sized images. This result is in compliance with the findings made in [13], where 64×64 sized image patches proved to give best performance in source camera identification.

Discussion An epoch represents the time taken for one forward pass and one backward pass of all the training examples. That is, when there are N training

Table 1. Classification accuracy results for binary classification between authentic and counter–forensic images. (Overall accuracy 93.4%)

		Predicted	
		Authentic	Counter–Forensic
Actual	Authentic	94.72%	5.28%
	Counter–Forensic	7.48%	92.52%

Table 2. Classification accuracy (%) among seam carved, fingerprint copied, and PRNU denoised images.

Image Size	32×32			64×64			128×128		
Batch Size	64	128	256	64	128	256	64	128	256
100 epochs	33.3	48.7	48.4	73.1	72.6	75.1	36.7	34.3	33.3
200 epochs	42.7	50.1	53.6	76.4	78.1	76.2	42.2	40.2	38.3
300 epochs	48.1	52.6	56.2	77.3	81.2	77.9	50.4	52.6	42.4
500 epochs	52.3	59.3	59.1	81.5	84.2	82.6	55.2	57.3	51.3
1000 epochs	55.7	61.2	60.2	84.6	**85.7**	84.1	59.2	61.2	56.4

samples and batches are of size b, then it takes $\frac{N}{b}$ iterations to complete one epoch. In our experiments, we varied the number of epochs until the performance of the proposed system stabilizes, and does not significantly change from one epoch to the next.

The image batch size also plays a crucial role in representation learning. It represents the number of samples that are going to be propagated through the deep learning model. Larger batch size implies higher memory requirement. For instance, if there are N training samples, and the batch size is fixed to be b, then sequential batches of $\frac{N}{b}$ samples are used iteratively for training the network. The advantage of using the concept of batches is that the entire dataset need not be loaded into memory at once. Also it makes the learning of the model faster, as the network weights are updated at every iteration.

In order to avoid overfitting, two dropout layers are used with values 0.2 and 0.5 respectively and we used a validation dataset to evaluate our performance (which is completely hidden from training) with 20% of total images. The classification accuracies presented in Table 1 and Table 2 are for the validation dataset. This proves that the proposed CNN architecture is capable of distinguishing between authentic and counter–forensic images with a considerably high efficiency; and it further detects the type of counter–forensic attack efficiently (with 64×64 images).

All the above mentioned parameters, viz., image size, batch size, number of epochs, kind of optimizer used (SGD in our case), hyperparameters like learning rate, momentum etc., decide the performance of a deep neural network.

5 Conclusion

In image source identification, the presence of counter–forensic images poses a serious threat to a forensic analyst, with respect to the credibility of the investigation results. Thus it is of paramount importance to identify whether an image is counter–forensically modified, and hence to remove those from the source identification module. In this paper, we perform a counter–forensic image classification, by adopting a two–level classification mechanism. At level one the proposed system distinguishes between authentic and counter–forensically

modified images. At level two, the counter–forensic images are further classified according to the source anonymization attack that they have undergone.

Future research in this direction would involve formulation of anti counter–forensic measures to combat the existing counter–forensic attacks, and hence to achieve highly accurate source identification, even with counter–forensic images.

References

1. Jessica Fridrich "Digital image forensics: there is more to a picture than meets the eye", *Springer*, 2012.
2. Mehdi Kharrazi, Hursre T. Sencar and Nasir Memon, "Blind Source Camera Identification", *International Conference on Image Processing (ICIP)* , 2004.
3. Oya Celiktutan, Bulent Sankur and Ismail Avcibas, "Blind Identification of Source Cell-Phone Model", *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3, Sep. 2008.
4. Seince Bayram, Husrev T. Sencar and Nasir Memon, "Improvements on Source Camera-Model Identification based on CFA Interpolation", *Proc. of WG*, 2006.
5. J Lukas, "Digital Camera Identification from Sensor Pattern Noise", *IEEE Transactions on Information Forensics and Security*, vol.1, issue:2, pp: 205–214, 2006.
6. Miroslav Goljan, Jessica Fridrich and Tomas Filler, "Large Scale Test of Sensor Fingerprint Camera Identification", *IS&T/SPIE Electronic Imaging*, pp: 72540I–72540I, 2009.
7. Chang–Tsun Li, "Digital Camera Identification from Sensor Pattern Noise", *IEEE Transactions on Information Forensics and Security*, vol.5, issue:2, 2010.
8. K.R. Akshatha, A.K. Karunakar, H. Anitha, U. Raghavendra and Dinesh Shetty, "Digital camera identification using PRNU: A feature based approach", *Digital Investigation, Elsevier*, vol. 19, pp: 69–77, 2016.
9. Bingchao Xu, XiaofengWang, XiaoruiZhou,JianghuanXi and ShangpingWang, "Source camera identification from image texture features", *Neurocomputing, Elsevier*, vol. 207, pp: 131–140, 2016.
10. Li Deng, Gen Lu, Yuying Shao, Minrui Fei and Huosheng Hu, "A novel camera calibration technique based on differential evolution particle swarm optimization algorithm", *Neurocomputing, Elsevier*, vol. 174, pp: 456–465, 2016.
11. Chen Chen and Matthew C. Stamm, "Camera Model Identification Framework Using An Ensemble of Demosaicing Features", *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015.
12. Amel Tuama, Frederic Comby and Marc Chaumont, "Camera Model Identification With The Use of Deep Convolutional Neural Networks", *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016.
13. Luca Bondi, Luca Baroffio, David Guera, Paolo Bestagini, Edward J. Delp and Stefano Tubaro, "First Steps Towards Camera Model Identification with Convolutional Neural Networks", *IEEE Signal Processing Letters* , vol. 24, Issue: 3, pp: 259–263, 2017.
14. S. Bayram, H. T. Sencar and N. D. Memon, "Seam-carving based anonymization against image and video source attribution", *in Proc. IEEE 15th Int. Workshop Multimedia Signal Process. (MMSP)* , 2013.
15. Ahmet Emir Dirik, Husrev Taha Sencar, and Nasir Memon, "Analysis of Seam-Carving-Based Anonymization of Images Against PRNU Noise Pattern-Based Source Attribution", *IEEE Transactions On Information Forensics And Security* , vol. 9, No. 12, 2014.

16. Erwin Quirring and Matthias Krichner, "Fragile sensor fingerprint camera identification", *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015.
17. Ahmet Karakk and Ahmet Emir Dirik, "Adaptive photo-response non-uniformity noise removal against image source attribution", *Digital Investigation, Elsevier*, vol.12, pp: 66–76, 2015.
18. Ahmet Karakuuk, Ahmet E. Dirik, Husrev T. Sencar and Nasir D. Memon, "Recent advances in counter PRNU based source attribution and beyond", *Proc. SPIE 9409, Media Watermarking, Security, and Forensics*, 2015.
19. Ashref Lawgaly, Fouad Khelifi, "Sensor Pattern Noise Estimation Based on Improved Locally Adaptive DCT Filtering and Weighted Averaging for Source Camera Identification and Verification", *IEEE Transactions on Information Forensics and Security*, vol.12, issue:2, pp:392–404, 2017.
20. Thomas Gloe and R. Bhme, "Dresden Image Database' for benchmarking digital image forensics", *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2010.
21. Thomas Gloe, "Feature-Based Forensic Camera Model Identification", *Transactions on Data Hiding and Multimedia Security VIII,Lecture Notes in Computer Science, vol 7228. Springer, Berlin, Heidelberg*, 2012.
22. Shai Avidan and Ariel Shamir, "Seam carving for content-aware image resizing", *ACM Transactions on Graphics (TOG)* , vol. 26, No. 10, Issue 3, 2007.
23. Hui Zeng, "Rebuilding the credibility of sensor-based camera source identification", *Multimedia Tools and Applications, Springer*, vol. 75, issue: 21, pp: 13871-13882, 2016.
24. Ian Goodfellow, Yoshua Bengio and Aaron Courville, "Deep Learning", http://www.deeplearningbook.org, MIT Press , 2016.
25. Rafael C Gonzalez and Richard E Woods, "Image Processing", Digital Image Processing, vol.2, 2007.
26. Bolei Zhou, Agata Lapedriza, Jianxiong Xiao,Antonio Torralba and Aude Oliva, "Learning deep features for scene recognition using places database", Advances in neural information processing systems, pp. 487–495, 2014.
27. Krizhevsky A.A, Sutskever I and Hinton G, "Imagenet classification with deep convolutional neural networks", Advances in Neural Information Processing Systems , pp. 1097-1105, 2012.
28. Francois Chollet, "Keras", https://github.com/fchollet/keras, 2015.