Detecting Counterfeit Bills and Their Forgery Devices using CNN-based Deep Learning

Soo-Hyeon Lee
Department of Computer Software Engineering
Kumoh National Institute of Technology
Daehak-ro 61, Gumi, Gyeongbuk, South Korea
e-mail: dark0487@naver.com

Hae-Yeoun Lee
Department of Computer Software Engineering
Kumoh National Institute of Technology
Daehak-ro 61, Gumi, Gyeongbuk, South Korea
e-mail: haeyeoun.lee@kumoh.ac.kr

***Abstract*—Counterfeit bills are easy to forge due to the advances in scanning and printing technologies. Individuals are less likely to find counterfeit bills. This paper proposes a deep learning-based algorithm to detect counterfeit bills and their forgery devices. The proposed algorithm has adopted a convolutional neural network model composed of 2 convolutional layers and 2 fully connected layers. In the convolutional layers, rectified linear unit and max-pooling are applied. In the fully connected layers, drop out is applied. To show the performance of the algorithm, experiments are performed using original bills and counterfeit bills forged with different manufacturers' printers. Nearly 100% detection accuracy has been achieved.**

Keywords-counterfeit bill detection; forgery device detection; deep learning; convolutional neural network.

I. INTRODUCTION

High performance scanning and printing devices can be accessed at low cost with the advances of IT (Information Technology). In addition, high quality image processing software has been developed. As a result, the general public can easily process complex tasks. However, novices can use these advanced technologies to create illegal products.

Credibility of currency is important in an economic society. Loss of currency credibility damages not only personal property but it also harms national creditworthiness. Recently, crimes forging counterfeit bills with high performance devices and high quality software are rapidly increasing.

Although various anti-counterfeiting technologies are applied to prevent counterfeiting such as magnetic stripe line, ultra violet watermark, and hologram pattern, counterfeit bill detectors require too high a cost and individuals are less likely to find counterfeit bills because too many bills are circulating.

To solve this problem, many counterfeit bill detection researches have been performed using tools such as ultra violet features, electro-magnetic features, and printing noise features. This paper focuses on research that uses printing noise features, where human beings have defined the features to discriminate between original bills and counterfeit bills. Then, these features were applied to the classifier. However, human beings have a limitation to define sophisticated features to discriminate between original bills and counterfeit bills.

This paper proposes a deep learning-based algorithm to detect counterfeit bills and their forgery devices. Since deep learning algorithms are not limited to human cognitive abilities, differently from human beings, the proposed algorithm can extract the sophisticated features by itself and hence robustly discriminate between original bills and counterfeit bills. The proposed algorithm has adopted a Convolution Neural Network (CNN) model, which is mainly used in image processing fields [1]. The model is composed of 2 convolutional layers having Rectified Linear Unit (ReLU) as an activation function and max-pooling and 2 fully connected layers having a drop-out function to prevent overfitting. Finally, a SoftMax function is used to rectify the results. Using original bills and counterfeit bills that are forged with 3 different color laser printers, experiments are performed. Nearly 100% accuracy in detecting counterfeit bills and their forgery devices has been achieved.

The paper is organized as follows. Section II reviews related works. The proposed algorithm is explained in Section III. Section IV shows experimental results and Section V concludes.

II. RELATED WORKS

To detect counterfeit bills, a lot of research is underway and its performance depends on how to extract accurately the unique characteristics of counterfeit bills that are different from the original bills. Among anti-counterfeiting technologies, the features used in previous studied algorithms are Ultra Violet (UV) features, electro-magnetic features, and printing noise features.

A. UV Features

UV features are easier to detect than other features. Chae et al. used the fact that UV information was only part of the bill [2]. Their algorithm improved accuracy and computation speed over conventional UV-based discrimination methods. After dividing the UV information extracted from the bill into 3x4 blocks, the difference from original bills was calculated to detect counterfeit bills. The detection rate of counterfeit bills was 100% and the accuracy of original bills was 99.3%.

Lee et al. proposed a speed optimized method to automatically detect UV information without using a conventional passive UV detection method [3]. The images obtained by UV illumination were separated by a Gaussian mixture model and Split-and-Merge EM (SMEM) algorithm.

Then, the size and weight of the covariance vector were considered to judge whether it was forged or not.

B. *Electrical Features*

Researches using electro-magnetic features of a printing material are also progressing steadily. Kang et al. proposed a counterfeit bill detection system by contacting a fiber optic sensor with a specific part of the bills [4]. In the bill, the area representing the amount of the bill was scanned through the optical fiber and the voltage measurement was used to make judgement. As a result, 100% accuracy was achieved in the test with Korean $50 bills.

C. *Printing Noise Features*

The noise features of printing devices can be used to detect counterfeit bills, and the algorithm proposed in this paper falls into this category. Ji et al. extracted non-local feature values and applied a support vector machine classifier to discriminate counterfeit bills [5]. Also, they identified printing devices to forge them. After extracting the noise factors of printing devices using a non-local averaging algorithm, feature values were extracted by calculating the Gray level co-occurrence matrix. Counterfeit bill detection accuracy was about 94% and their forged device detection accuracy was about 93%.

Baek et al. proposed an algorithm using low resolution multispectral images, where human readable features such as optically variable ink and machine readable features by multi-channel IR (Infra Red) hardware sensors are combined to discriminate counterfeit bills from original bills [6]. They achieved 100% detection accuracy for counterfeit bills with 99.8% classification accuracy.

There are other studies to detect printing devices. Lee et al. used a Wiener filter to extract the noise feature of printing devices, which was useful for removing abnormal noise [7]. Since printers converted the RGB (Red, Green, Blue) channels of images to the CMYK (Cyan, Magenta, Yellow, Black) channels for printing, the scanned image having the RGB channels was transformed into the CMYK channels. Then, the printing noise was extracted by calculating the difference between the image and its Wiener-filtered image and was used as the feature.

Choi et al. and Baek et al. used high-frequency components that were extracted by discrete wavelet transform as the printing noise feature [8] [9].

Ryu et al. studied a printing device detection algorithm considering that color laser printers had a unique pattern for CMYK printing [10]. The directional information of the linear characteristics existing in the printing pattern was extracted using Hough transform and was used as the feature.

Against mistreated Mexican bills, not counterfeit bills, Garcia-Lamont et al. proposed a classification method, where their color and local binary patterns from texture features are used [11].

However, in these algorithms, there are disadvantages that human beings must design a method to extract features and there are limitations in designing the sophisticated way to extract features for distinguishing between original bills and counterfeit bills.

III. Proposed CNN-based Detection Algorithm

In order to detect counterfeit bills and their forgery devices, a deep learning-based algorithm based on CNN has been proposed, which consists of two steps: training and testing. Figure 1 shows the overall process of the algorithm. Using training data, the proposed model is trained and the accuracy is evaluated by comparing with the label of the training data. Then, the weights and biases of the model are updated via error back propagation with reference to the accuracy. After learning a certain number of times, testing data are applied to the model and detection results are analyzed to calculate the accuracy.

Deep learning is a neural network that has deeper layer than existing artificial neural networks. According to recent studies, the CNN model among various deep learning models is suitable for image processing applications and can extract sophisticated features to achieve high performance without human intervention [1].

Therefore, the proposed algorithm to detect counterfeit bills and their forgery device is designed using this CNN model. In general, the CNN model consists of an input layer, a convolutional layer, a fully connected layer, and an output layer.

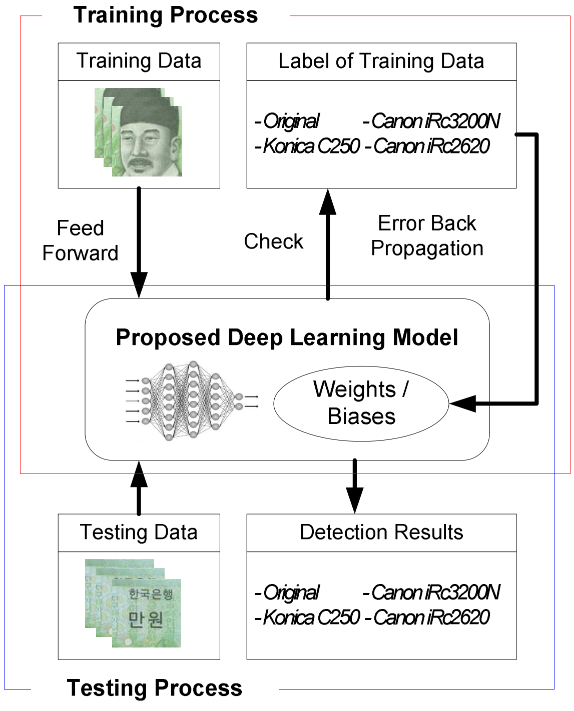

Figure 1. Counterfeit bills and their forgery device detection process

Generally, the convolutional layer includes a convolution operation, a pooling operation, and an activation function. The convolution operation can extract features considering the values of local pixels by a matrix operation of image and filter. The pooling operation leaves only pixel values that satisfy certain rules among the pixels in a specific area. This can reduce the size of the input data and improve the processing speed. However, it can lose important pixel values that can contribute to identify counterfeit bills. When linear results are used, normal learning is difficult due to the problem of vanishing gradients in the back propagation process. Therefore, an activation function is used to nonlinearly change the results of the previous layer.

The fully connected layer is the most basic component of an artificial neural network. The data from the previous layer are used as input nodes one by one and fully connected to the output nodes. Overfitting is a situation in which too much data are learned for a particular dataset and hence fails to provide adequate results for additional data. To prevent overfitting, drop-out is a normalization technique, which drops random nodes of fully connected layer nodes during the learning process [12]. Differently from our previous research, which just focused on differentiating between original bills and counterfeit bills [13], the output layer is composed of 4 nodes to identify forgery devices and parameters are tuned to improve the performance.

The output values of the fully connected layer can be varied in range. To rectify the values, a SoftMax function is applied in the output layer.

The detail of the proposed CNN-based model is depicted in Figure 2, which consists of 4 layers: an input layer, a convolutional layer, a fully connected layer, and an output layer.

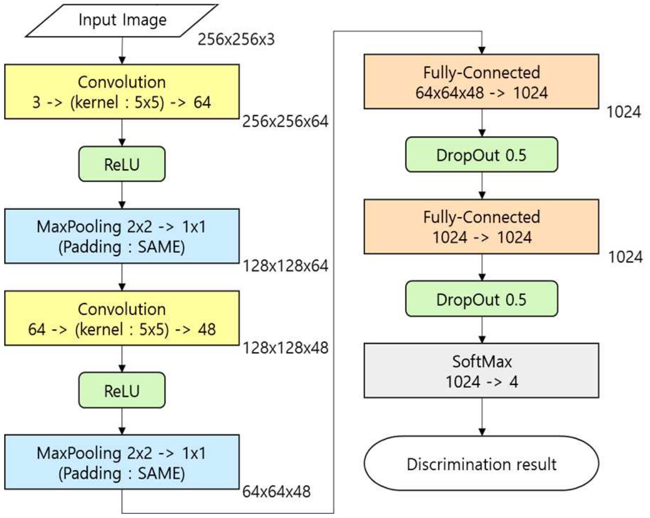

Figure 2. Details of the proposed CNN-based model

The input layer and the output layer are matched to an input image and discrimination result, respectively. The initial values of weights and biases were adjusted.

The 1st convolutional layer receives 256x256 color images having RGB channels and outputs 64 feature maps by convolving a 5x5 kernel. ReLU is used as an activation function and the 256x256 size of feature maps is reduced to the 128x128 size of feature maps through max-pooling with stride 2. The 2nd convolutional layer receives 64 feature maps as an input and outputs 48 feature maps. The same activation function is used as the first layer and max-pooling with stride 2 reduces the 128x128 size of feature maps to the 64x64 size of feature maps.

256x256 color images having RGB channels become 48 feature maps having a 64x64 size through 2 convolutional layers. Then, these feature maps are rearranged into a one-dimensional array with 64x64x48 values.

Through the 1st fully connected layer, these values are output to 1024 nodes, where a drop-out processing of 0.5 rate is applied to prevent overfitting. Also, through the 2nd fully connected layer, the discrimination result is acquired after rectifying the value with the SoftMax function.

IV. Experimental Results

For the experiment, original bills are scanned to make original bill images. Then, counterfeit bills are created by printing these original bill images and scanned again to get the counterfeit bill images. As printers for counterfeiting, we used Konica C250, Canon iRc3200N, and Canon iRC2620 color laser printers.

Due to the memory limitation of deep learning hardware, it is impossible to use the scanned bill images directly. Therefore, scanned bill images are randomly cropped with 100 images of 256x256 size. Since the data ratio of the original bill images and the counterfeit bill images is 1:3, up-sampling is performed to 300 original bill images.

The entire data consists of 10,800 (36x300) original bills and 10,800 (36x100x3 printers) counterfeit bills. The ratio of the training data to the testing data is 8:2, i.e., 8,640 and 2,160, respectively. Figure 3 shows original bill images and counterfeit bill images generated by each printing device.

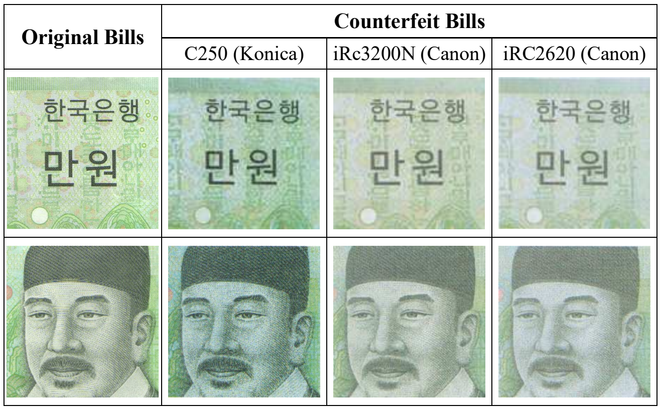

Figure 3. Original bill images and counterfeit bill images with each device

A. Detection Accuracy

The detection accuracy of original bills, counterfeit bills and their forgery device is analyzed to show the performance of the proposed algorithm. The results are depicted in Figure 4 and summarized in Table I. In Figure 4, a horizontal axis represents the number of epochs and a vertical axis indicates the detection accuracy. In Table I, the last column (All) is the average of detection accuracy for 3 printers.

As shown in the results, the detection accuracy increases with the increase of epochs. After 25 epochs, the detection rate of original bills and counterfeit bills is 100%. Also, the detection of their forgery device is 100%. It means that the proposed algorithm using CNN-based deep learning can extract the sophisticated features for discriminating original bills and counterfeit bills. Also, it can discriminate the differences among their forgery devices.

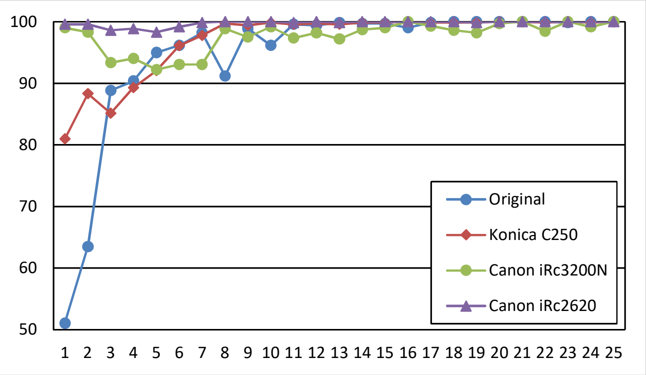

Figure 4. Counterfeit bill forgery device detection accuracy

TABLE I. DETECTION ACCURACY OF COUNTERFEIT BILLS AND THEIR FORGERY DEVICE (PER EPOCH)

Epoch	Original	Counterfeit Bills and Forgery Device			
		C250 (Konica)	iRc3200N (Canon)	iRc2620 (Canon)	All
1	51.02	80.97	99.03	99.58	93.19
2	63.47	88.33	98.33	99.58	95.41
3	88.84	85.14	93.33	98.61	92.36
4	90.37	89.31	94.03	98.89	94.08
5	95.00	92.08	92.22	98.33	94.21
6	96.16	96.11	93.06	99.17	96.11
7	98.19	97.78	93.06	99.86	96.90
8	91.20	99.72	98.89	100.00	99.54
9	98.89	99.44	97.50	100.00	98.98
10	96.16	99.86	99.17	100.00	99.68
11	99.58	99.58	97.36	99.86	98.93
12	99.44	99.72	98.19	100.00	99.30
13	99.86	99.58	97.22	99.86	98.89
14	99.72	99.86	98.75	100.00	99.54
15	99.72	99.86	99.03	100.00	99.63
16	99.07	100.00	100.00	100.00	100.00
17	99.86	99.86	99.31	100.00	99.72
18	100.00	99.86	98.61	100.00	99.49
19	100.00	99.86	98.19	99.86	99.30
20	100.00	100.00	99.72	100.00	99.91
21	100.00	100.00	100.00	100.00	100.00
22	100.00	99.86	98.47	100.00	99.44
23	99.86	100.00	100.00	100.00	100.00
24	100.00	99.86	99.17	100.00	99.68
25	100.00	100.00	100.00	100.00	100.00

V. CONCLUSION

As scanning and printing devices are improved and costs are reduced, counterfeit bills are made easier than ever. As a result, counterfeit bills have been circulated in various ways, and anti-counterfeiting technologies have been studied to prevent counterfeiting crimes.

In this paper, we proposed a CNN-based deep learning algorithm that could detect counterfeit bills and their forgery devices. Also, we performed intensive experiments to show the outstanding performance. The proposed algorithm could achieve 100% accuracy in discriminating between original bills and counterfeit bills. Also, it could identify their forgery devices with 100% accuracy.

In the experiments, contaminated bills commonly found in practice are not considered. Therefore, it is necessary to perform additional studies for commonly used damaged and contaminated bills. Also, we consider increasing the depth of the model or including pre-processing filters. Therefore, there are many opportunities to research.

ACKNOWLEDGMENT

This work was partly supported by the research fund of National Security Research (2018-069).

REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, “Deep Learning,” Nature, vol. 521, pp. 436-444, 2015.

[2] S. H. Chae, T. Y. Seo, and S. B. Pan, “The Study for Authenticity Distinguish of Banknote using UV Information,” Proceedings of KIIT Summer Conference, 2009, pp. 753-756.

[3] G. H. Lee and T. H. Park, “Automatic Extraction of UV patterns for Paper Money Inspection,” Journal of Korean Institute of Intelligent Systems, vol. 21 (3), pp. 365-371, 2011.

[4] D. H. Kang and J. H. Hong, “A Study about the Discrimination of Counterfeit ₩50,000 bills Using Optical Fiber Sensor,” Journal of Korean Society of Manufacturing Technology Engineers, vol. 21 (1), pp. 15-20, 2012.

[5] H. Y. Lee and S. G. Ji, “Counterfeit Money Detection Algorithm using Non-Local Mean Value and Support Vector Machine Classifier,” Journal of KIPS Transactions on Software and Data Engineering, vol. 2 (1), pp. 55-64, 2013.

[6] S. Baek, E. Choi, Y. Baek, and C. Lee, “Detection of Counterfeit Banknotes using Multispectral Images,” Digital Signal Processing, pp. 1-11, 2018, in press.

[7] H. Y. Lee, J. Y. Baek, S. G. Kong, H. S. Lee, and J. H. Choi, “Color Laser Printer forensics through Wiener Filter and Gray Level Co-occurrence Matrix,” Journal of Korea Institute of Information Scientists and Engineers, vol. 37 (8), pp. 599-610, 2010.

[8] J. H. Choi, H. Y. Lee, and H. K. Lee, “Color Laser Printer Forensics based on Noisy Feature and Support Vector Machine Classifier,” Multimedia Tools and Applications, vol. 67 (2), pp. 363-382, 2013.

[9] J. Y. Baek et al., “Color Laser Printer Identification through Discrete Wavelet Transform and Gray Level Co-occurrence Matrix,” Journal of KIPS Transactions on Software and Data Engineering, vol. 17 (3), pp. 197-206, 2010.

[10] S. J. Ryu, H. Y. Lee, D. H. Im, J. H. Choi, and H. K. Lee, “Electrophotographic Printer Identification by Halftone Texture Analysis,” Proceedings of IEEE International

Conference on Acoustics Speech and Signal Processing (ICASSP), 2010, pp. 1846-1849.

[11] F. Garcia-Lamont, J. Cervantes, and A. Lopez, “Recognition of Mexican Banknotes via Their Color and Texture Features,” Expert Systems with Applications, vol. 39, pp. 9651-9660, 2012.

[12] N. Srivastava, G. E. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: A Simple Way to Prevent Neural Networks from Overfitting,” Journal of Machine Learning Research, vol. 15 (1), pp. 1929-1958, 2014.

[13] S. H. Lee and H. Y. Lee, “Counterfeit Bill Detection Algorithm using Deep Learning,” International Journal of Applied Engineering Research, vol. 13 (1), pp. 304-310, 2018.