International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 304-310

Counterfeit Bill Detection Algorithm using Deep Learning

Soo-Hyeon Lee[1] and Hae-Yeoun Lee[2],*

[1]Undergraduate Student, [2]Professor
[1,2] Department of Computer Software Engineering,
Kumoh National Institute of Technology, 61 Daehak-ro, Gumi, Gyeongbuk, 39177, South Korea.
**Corresponding author*

ORCIDs: [1]0000-0002-3372-5660, [2]0000-0002-6081-1492

Abstract

The advance of scanner and printer technologies has increased the possibility of making counterfeit bills that cannot be distinguished by human and simple detecting devices. The rate of finding counterfeit bills by individuals is very low because counterfeit bill detectors require too high a cost. In this paper, we propose a deep learning-based algorithm to detect counterfeit bills through general-purpose scanners that can be used by individuals to prevent personal monetary damages caused by counterfeit bills. The proposed algorithm adopts a convolutional neural network model that consists of 2 convolutional layers and 2 fully connected layers. In convolutional layers, rectified linear unit and max-pooling are applied. In fully connected layers, drop out is applied. Using original bills and counterfeit bills printed by various manufacturers' printers, experiments are performed. Also, the proposed algorithm is compared with previous feature-based algorithms to show the outstanding performance.

Keywords: Counterfeit bill detection, Deep learning, Convolutional neural network

INTRODUCTION

The advance of computers and digital devices makes high-performance imaging and scanning devices to be accessed at low cost. High-quality image processing software has also been developed to produce high-quality images. As a result, the general public can easily process complex tasks. However, novice can use these advanced technologies to create illegal counterfeit bills.

Currency is common means of exchange or general circulation to facilitate the exchange and distribution of goods in the exchange economy society. Currency credibility is important as means of economic society since it not only damages personal property but also harms national creditworthiness. Recently counterfeiting crimes are rapidly increasing in forgery crimes. Counterfeiting crime is not just a matter of one country. Therefore, detecting counterfeit bills is helpful for the soundness of the economy and society.

As shown in Fig. 1, the damage to monetary counterfeiting crime is the second highest in transnational crime anticipated. Also, India has blocked the use of high-value bills to prevent counterfeit bills. However, as shown in Fig. 2, it is not easy for individuals to find counterfeit bills like the contents.

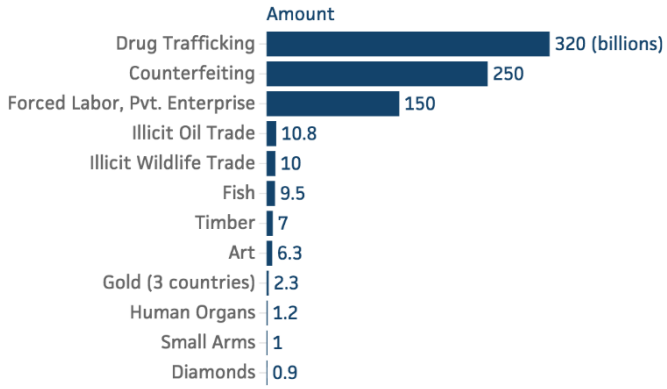


Figure 1. Estimated revenues for illicit trade by sector (World Economic Forum, 2011)

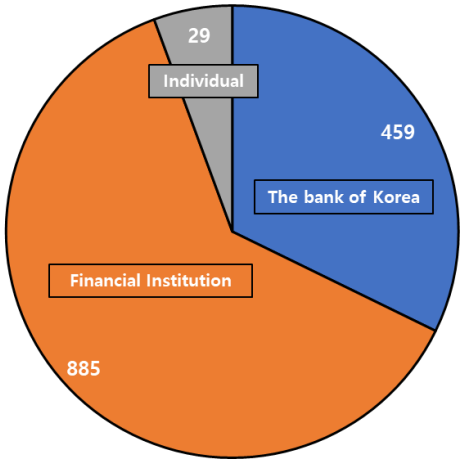


Figure 2. Detection of counterfeit bills by discoverer in Korea (Bank of Korea, 2016)

To prevent counterfeiting crime, various anti-counterfeiting technologies are applied, such as magnetic stripe line, ultraviolet watermark, and hologram pattern. Nevertheless, it is difficult to check for counterfeit bills every time because too many bills are circulating, and imaging and scanning technologies advance. Also, counterfeit bill detectors require too high a cost. That is why it is difficult for individuals to find counterfeit bills.

As a method to solve this problem, feature-based counterfeit bill detectors have studied, where human extracted the feature to discriminate original bills and counterfeit bills. This extracted feature was applied to the classifier. However, human has a limitation to extract the sophisticated features to discriminate original bills and counterfeit bills.

In this paper, we propose a deep learning-based algorithm to detect counterfeit bills using a general-purpose canner. The proposed algorithm adopts a convolutional neural network model that consists of 2 convolutional layers and 2 fully connected layers. Differently from human, deep learning algorithms are not limited to human cognitive abilities. As a result, the algorithm can extract the sophisticated features by itself and hence robustly discriminate original bills and counterfeit bills. The proposed algorithm adopts a convolution neural network (CNN) model which is mainly used in image processing fields. The model is composed of 2 convolutional layers having max-pooling and rectified linear unit (ReLU) as an activation function and 2 fully connected layers having a drop-out function to prevent overfitting. Finally, a SoftMax function is used to rectify the results. Experiments are performed with original bills and counterfeit bills that are created with 3 different color laser printers. The proposed algorithm outperforms over other previous feature-based algorithms.

The paper is organized as follows. Sec. 2 reviews related works. The proposed algorithm is explained in Sec.3. Sec. 4 shows experimental results and Sec. 5 concludes.

RELATED WORK

Many researches to detect counterfeit bills are underway. The performance of counterfeit bill detection algorithms depends on the way to accurately extract the unique characteristics of the counterfeit bills differently from original bills. Among anti-counterfeiting technologies, the features used in the existing algorithms are ultra violet (UV) features, electromagnetic features, and printing noise features.

UV Features

UV features are easier to detect than other features. Various counterfeit bill detection algorithms using UV features have been studied. Chae et. al used the fact that UV information is only part of the bill [1]. 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 with the original bill was calculated to detect the counterfeit bills. As a result, the detection rate of counterfeit bills was 100% and the accuracy of original bills was 99.3%.

To optimize the speed performance, Lee et al. proposed a method to automatically detect UV without using a conventional passive UV detection method [2]. The images obtained by UV illumination are separated by a Gaussian mixture model and Split-and-Merge EM (SMEM) algorithm. Then, the size and weight of the covariance vector were considered and judged whether it was forged or not. As a result, the detection time was reduced compared to the conventional method.

Electrical Features

Researches using an electromagnetic feature of a printing material rather than an optical feature are also progressing steadily. Kang et al. proposed a system for detecting between counterfeit bills by contacting a fiber optic sensor with a specific part of the bills [3]. The area representing the amount of the bill was scanned through the optical fiber and the voltage measurement was used to judge whether it was a counterfeit bill. As a result, 100% accuracy was achieved in the test with Korean $50 bills.

Printing Noise Features

Researches using noise features of printing devices are also under way. Ji et al. extracted the non-local feature values and applied the support vector machine classifier to discriminate bills [4]. Also, they identified printing devices to make counterfeit bills. After extracting the noise of printing devices using the non-local averaging algorithm, feature values of noise were extracted using the Gray level co-occurrence matrix. Their detection performance of counterfeit bills was about 94% and the detection accuracy of printing devices is about 93%.

The use of printing noise features is not limited to detect counterfeit bills. There have been many 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 [5]. Since printers convert the RGB channels of images to the CMYK channels for printing, the scanned image having the RGB channels has transformed into the CMYK channels. Then, the printing noise was extracted by calculating the difference between the image and its Wiener-filtered image and used as a feature.

To identify printing devices, Choi et al. and Baek et al. used high-frequency components extracted by discrete wavelet transform as printing noise features [6] [7]. Ryu et al. studied a printing device detection algorithm considering that color laser printers have a unique pattern for CMYK printing [8]. The directional information of the linear characteristics existing in the print pattern was extracted using Hough transform and used as a feature. However, in these algorithms, there are disadvantage that human has to design a method to extract features and has a limitation to design the sophisticated way to extract features.

PROPOSED DEEP LEARNING ALGORITHM

Deep learning background knowledge

Deep learning is a neural network that has deeper layer than existing artificial neural networks. Representative deep learning models include deep neural network (DNN) used for general data processing, convolution neural network (CNN) using convolution layer and pooling for image and audio information processing, and recurrent neural network (RNN)

for time series information processing [9].

According to recent studies, CNN is suitable for image processing applications. In this study, a counterfeit bill detection model was designed using this CNN. In general, CNN consists of an input layer, a convolution layer, a fully connected layer, and an output layer as shown in Figure 3.

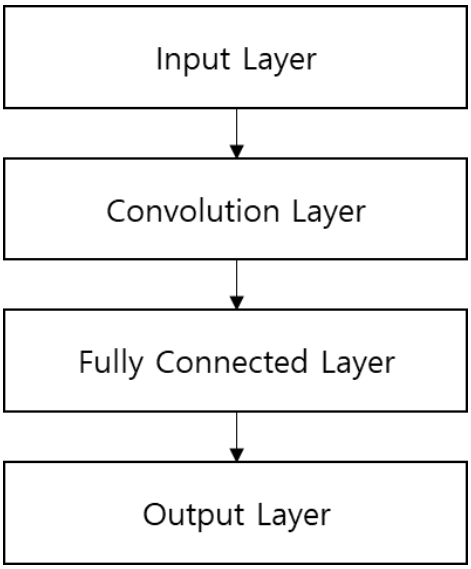
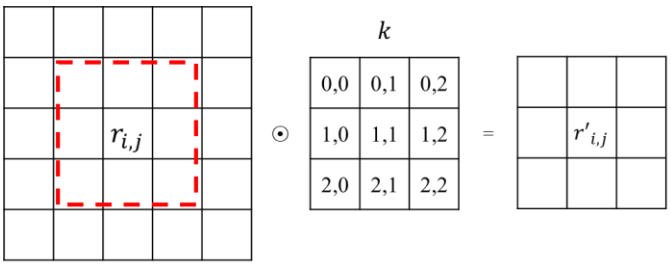


Figure 3. Basic layers of the CNN model

The convolution layer generally 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 convolution operation is depicted in Figure 4.



$$r'_{i,j} = r_{i-1,j-1} \times k_{0,0} + r_{i-1,j} \times k_{0,1} + r_{i-1,j+1} \times k_{0,2} + \cdots + r_{i+1,j-1} \times k_{2,0} + r_{i+1,j} \times k_{2,1} + r_{i+1,j+1} \times k_{2,2}$$

Figure 4. Convolution operation

The pooling operation leaves only pixel values that satisfy certain rules among the pixels in a specific area. This reduces the size of the input data and improves the processing speed. In general, max-pooling and average-pooling are commonly used. However, instead of speeding up processing, we can lose important pixel values that can be contribute to identify counterfeit bills. Figure 5 shows an example of max-pooling.

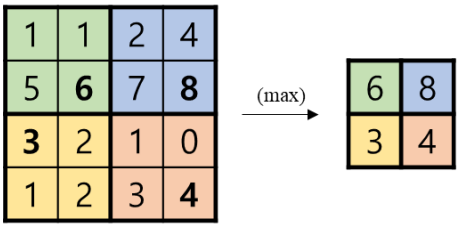


Figure 5. Max-pooling with stride 2

Activation is used to nonlinearly change the results of the previous layer. When linear results are used, normal learning is difficult due to the problem of vanishing gradient in the back propagation process. Generally, ReLU, Sigmoid, and tanh functions are used.

The fully connected layer is the most basic component of DNN. The data from the previous layer is used as input nodes one by one and fully connected to the output nodes. Drop-out is a normalization technique to prevent overfitting. Overfitting is a situation in which too much data is learned for a particular dataset, failing to provide adequate results for additional data. To prevent this, drop-out processing drops random nodes of fully connected layer nodes during the learning process [10].

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

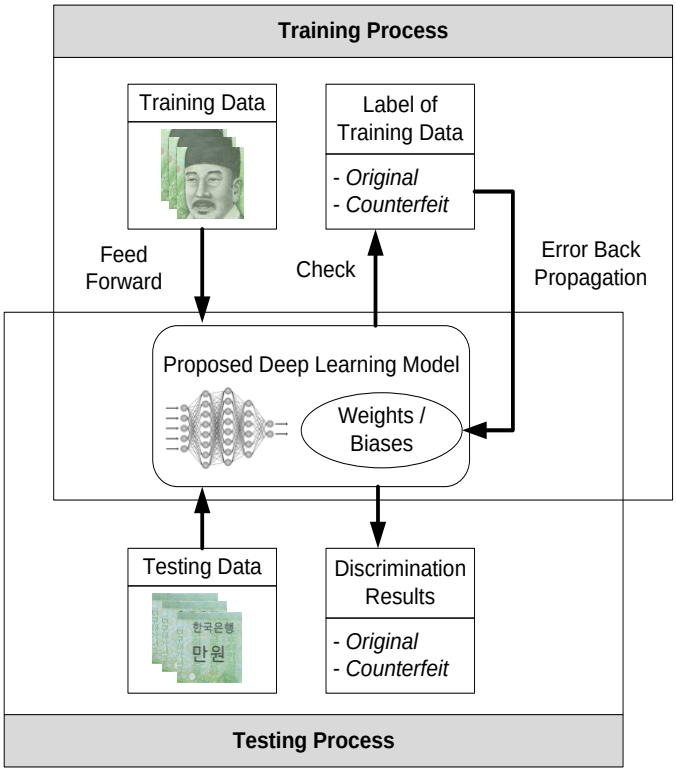


Figure 6. Overall counterfeit bills detection algorithm

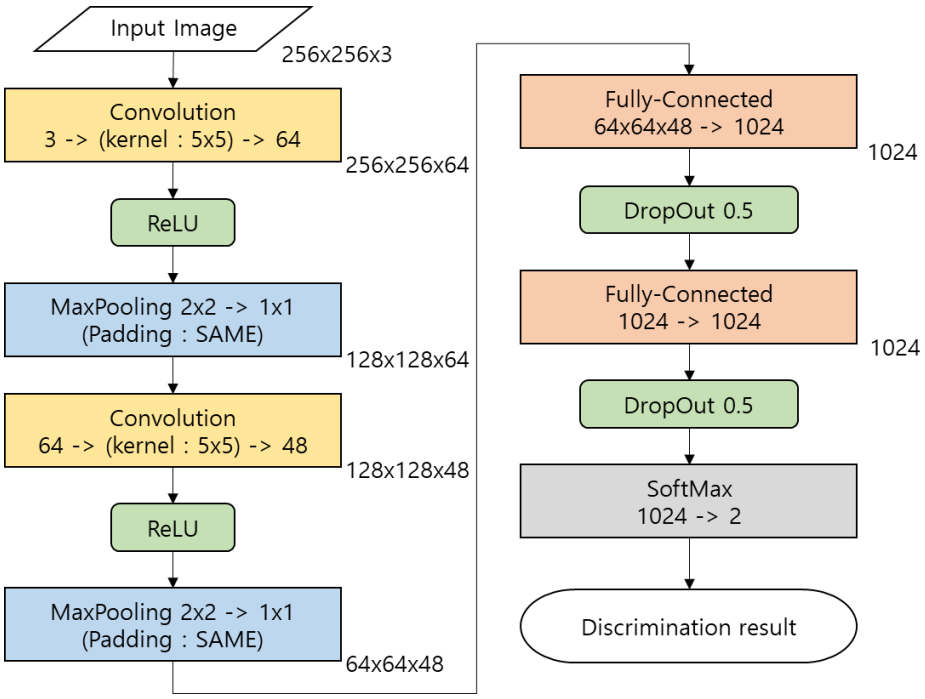


Figure 7. Deep learning model based on CNN

Deep Learning-based Counterfeit Bill Detection Algorithm

The proposed deep learning-based algorithm to detect counterfeit bills consists of two steps: training and testing. Figure 6 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, weights and biases are updated via error back propagation with the reference to accuracy. After learning a certain number of times, testing data is applied to the model and detection results are analyzed to calculate the accuracy.

The proposed deep learning model is depicted in Figure 7, which is composed of 4 layers: input layer, convolutional layer, fully connected layer, and output layer. The input layer and the output layer are matched to input image and discrimination results, 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 map is reduced to the 128x128 size of feature map 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 becomes 48 feature maps having 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.

EXPERIMENTAL RESULTS

Training and Testing Data

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 printers. These printers are color laser printers capable of high-quality printing.

Due to the memory limitations of deep learning hardware, it is impossible to use the scanned bill images directly. Also, it is difficult to produce a large amount of original and counterfeit bill images. Therefore, bill images are processed as follows to generate many data samples. First, the scanned bill images were divided into 36 parts and each image was randomly cropped with 100 images of 256x256 size. However, since the data ratio of the original bill images and the counterfeit bill images is 1:3, up-sampling was performed to 300 images.

The whole 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 and 8,640 and 2,160, respectively. Figure 8 shows original bill images and counterfeit bill images generated by each printing device.

Device (Brand)	Original bills	Counterfeit bills		
		C250 (Konica)	iRc3200N (Canon)	iRC2620 (Canon)
Sample #1				
Sample #2				

Figure 8. Original bill images and counterfeit bill images with each printing device.

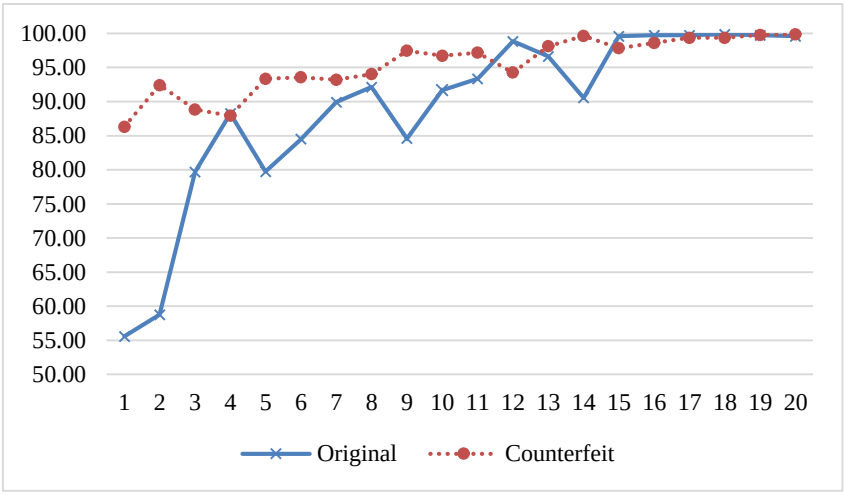


Figure 9. Detection accuracy (per epoch)

System Environment

The deep learning model for the detection of counterfeit bills was performed on hardware specifications and software environments as shown on Table 1 and Table 2. The latest specification of hardware such as CPU and graphics cards was utilized. The software platform was Google TensorFlow version 1.4.0 in Windows environment.

Table 1: Hardware specifications

Item	Specification.
CPU	Intel i7-7700
VGA	NVIDIA Titan Xp D5X 12GB
RAM	16GB (8GB * 2)

Table 2: Software environment

Item	Environment
OS	Windows 10 Pro
CUDA / cuDNN	8.0 / 5.1
Python	3.5
TensorFlow	1.4.0 (ver. GPU)

Analysis Results

The counterfeit bill detection results using the proposed model are depicted in Figure 9 and summarized in Table 3. In the Figure, the horizontal axis represents the number of epochs and the vertical axis indicates the detection accuracy. The detection accuracy increases with the increase of epochs. After 30 epochs,

the detection rate of original bills and counterfeit bills was 100%. It means that the proposed algorithm based on deep learning can extract the sophisticated feature for discriminating original bills and counterfeit bills.

Table 4 summarized the detection results of previous feature-based counterfeit detection algorithms [4]. To extract features, wiener filter, discrete wavelet transformation, and non-local averaging value were used, that were reviewed in related works. The average accuracy was 89.50%, 87.40%, and 94.24% respectively.

Table 3: Detection accuracy results (per epoch)

Epoch	Original	Counterfeit	Epoch	Original	Counterfeit
1	49.26	93.01	16	99.31	99.86
2	63.61	95.05	17	100	99.31
3	86.81	92.27	18	100	99.12
4	87.92	93.61	19	100	98.75
5	94.40	94.31	20	100	99.86
6	95.42	95.79	21	100	99.95
7	98.43	96.71	22	100	99.03
8	91.99	99.12	23	100	100
9	98.84	98.19	24	100	99.40
10	96.71	99.21	25	100	100
11	100	98.15	26	100	100
12	100	98.75	27	100	100
13	100	98.38	28	100	100
14	100	98.94	29	100	100
15	100	99.26	30	100	100

Table 4: Accuracy of previous feature-based detection algorithm

	Wiener filter	Discrete Wavelet Transform	Non-local averaging
1	90.43	85.19	94.14
2	87.35	86.42	94.75
3	92.90	88.27	93.83
4	90.74	87.35	94.75
5	88.89	88.27	92.90
6	86.73	88.89	95.06
Average	89.50	87.40	94.24

The proposed deep learning-based algorithm has improved the detection accuracy by more than 5% on average compared to previous feature-based detection algorithm. For some feature extraction algorithm, the proposed algorithm shows a large difference of more than 10%. Figure 10 have compared these accuracy in a graph.

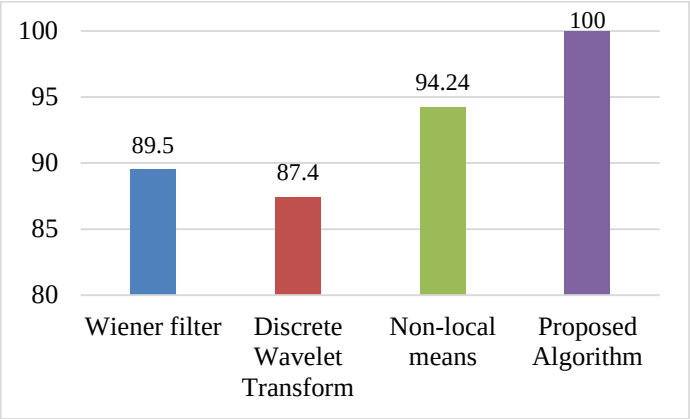


Figure 10. Accuracy comparison of algorithms

CONCLUSION

As scanning and printing devices have improved while lowering costs, counterfeit bills are made easier than ever before. As a result, counterfeit bills have been circulated in various ways, and anti-counterfeiting technology has been studied to prevent counterfeiting crimes. However, there is still a fight between counterfeiting and evasion techniques.

In this paper, we proposed a deep learning-based algorithm that could detect high-quality counterfeit bills using a general-purpose scanner. We have designed a convolutional neural network model for detecting the counterfeit bills and performed intensive experiments to show the outstanding performance of deep learning compared with previous algorithms. The proposed algorithm could improve the performance up to 10% compared to previous feature-based algorithms. Although the model was trained within a limited number of images, it showed 100% accuracy in fast. Through these results, we showed that deep learning could extract the sophisticated features very well to discriminate original bills and counterfeit bills and overcome the limitation of previous algorithms requiring human intervention.

In the experiments, contaminated bills commonly found in practice were not considered. Therefore, it is necessary to perform additional studies for commonly used damaged and contaminated bills. We consider including pre-processing filters or increasing the depth of the model. Also, with the detection of counterfeit bills, it will be useful for crime investigation if we can identify the printing device to make counterfeit bills. Therefore, there are many opportunity to research.

Acknowledgment

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03030432).

REFERENCES

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

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

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

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

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

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

[7] Baek, J. Y., Lee, H. S., Kong, S. G., Choi, J. H., Yang, Y. M., and Lee, H. Y., 2010, "Color Laser Printer Identification through Discrete Wavelet Transform and Gray Level Co-occurrence Matrix," Journal of KIPS Transactions on Software and Data Engineering, 17(3), pp. 197-206.

[8] Ryu, S. J., Lee, H. Y., Im, D. H., Choi, J. H., and Lee, H. K., 2010, "Electrophotographic printer identification by halftone texture analysis," Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), pp. 1846-1849.

[9] Schmidhuber, J., 2015, "Deep learning in neural networks: An overview," Neural networks, 61, pp. 85-117.

[10] Srivastava, N., Hinton, G. E., Krizhevsky, A., Sutskever, I., and Salakhutdinov, R., 2014, "Dropout: a simple way to prevent neural networks from overfitting," Journal of Machine Learning Research, 15(1), pp. 1929-1958.