JURNAL NASIONAL TEKNIK ELEKTRO DAN TEKNOLOGI INFORMASI
p-ISSN 2301–4156 | e-ISSN 2460–5719

CNN-Based Model for Copy Detection Pattern Estimation and Authentication

Syukron Abu Ishaq Alfarozi[1], Azkario Rizky Pratama[2]

[1,2] Department of Electrical and Information Engineering, Faculty of Engineering Universitas Gadjah Mada, Yogyakarta 55281 INDONESIA (tel.: 0274-5555; fax: 0274-4321; email: [1]syukron.abu@ugm.ac.id, [2]azkario@ugm.ac.id)

[Received: 29 November 2022, Revised: 24 January 2023]
Corresponding Author: Syukron Abu Ishaq Alfarozi

ABSTRACT — Counterfeiting has been one of the crimes of the 21st century. One of the methods to overcome product counterfeiting is a copy detection pattern (CDP) stamped on the product. CDP is a copy-sensitive pattern that leads to quality degradation of the pattern after the print and scan process. The amount of information loss is used to distinguish between original and fake CDPs. This paper proposed a CDP estimation model based on the convolutional neural network (CNN), namely, CDP-CNN. The CDP-CNN addresses the spatial dependency of the image patch. Thus, it should be better than the state-of-the-art model that uses a multi-layer perceptron (MLP) architecture. The proposed model had an estimation bit error rate (BER) of 9.91% on the batch estimation method. The error rate was 9% lower than the previous method that used an autoencoder MLP model. The proposed model also had a lower number of parameters compared to the previous method. The effect of preprocessing, namely the use of an unsharp mask, was tested using a statistical testing method. The effect of preprocessing had no significant difference except in the batch estimation scheme where the unsharp mask filter reduced the error rate by at least 0.5%. In addition, the proposed model was also used for the authentication method. The authentication using the estimation model had a good separation distribution to distinguish the fake and original CDPs. Thus, the CDP can still be used as the authentication method with reliable performance. It helps anti-counterfeiting on product distribution and reduces negative impacts on various sectors of the economy.

KEYWORDS — Copy Detection Pattern, Convolutional Neural Network, Anti-Counterfeiting.

I. INTRODUCTION

Counterfeiting is an infringement of an owner of intellectual property and is a crime that negatively impacts various sectors of the economy. Many have even referred to the crime of the 21st century [1], [2]. The Organization for Economic Cooperation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) published a joint report in 2019 on the trends in trade in counterfeit and pirated goods based on 2016 world seizure data [1], [3]. They found that trade in counterfeit and pirated goods amounted to $509 billion (3.3% of world trade). As of 2013, this number has increased to 461 billion dollars (2.6% of world trade). It increased even when overall world trade experienced a relative slowdown, more over this number only represented seized products and did not represent the full extent of counterfeit's impact on all sectors of the economy, including producers of genuine goods, customers, and governments.

Counterfeited goods directly affected the selling of their original products. Companies worldwide lose billions of dollars every year to counterfeiters. According to the secretary general of the International Chamber of Commerce (ICC), multinational manufacturers lost an estimated 10% of their top-line revenue to counterfeiters [1].

Battling counterfeiters require the involvement and commitment of all parties involved. Mike O'Neil, Secretary of ISO/TC 247 on fraud countermeasures and controls states that the combat against counterfeiting is done in four primary areas: (1) legislative actions to protect intellectual properties and penalize counterfeiting, (2) national customs organizations to prevent counterfeit entering their country, (3) private industry efforts to create anti-counterfeiting technology, and (4) national and international standards being developed [1].

Being the ones affected the most, companies producing genuine goods will have to develop their approach to protect the authenticity of their product. Various technologies have been implemented to achieve secure product protection. Each is different by cost, sophistication, and effectiveness in detecting a counterfeit. Technologies frequently implemented include holograms, smart cards, biometric markers and inks, and copy detection patterns (CDPs) [4].

CDP is one of the solutions developed to battle counterfeiting. CDP is a copy-sensitive digital image with a specific property that will be printed and embedded into the products. CDP detects authentic and counterfeited products by relying on the information loss principle [5]. On every Print-and-Scan (P&S) process of a digital image, some information will be lost due to image degradation and noise will be added from the printing process. Hence, every time an image is printed or processed, there will be structural and quality changes to the resulting image. It will be different from CDP's first print, which can only be found on authentic products. P&S is a stochastic process with a random probability distribution that can be analyzed statistically, but it is hard to predict. CDP generates an image with unpredictable content to prevent counterfeiters from improving explicit and implicit knowledge of the image. Images that store maximum information such as noise-like images are the hardest to replicate. This kind of images can be achieved by assigning a totally random and unpredictable value to each pixel. It then can be concluded that the most challenging image to replicate is an image composed of pure noise, which has maximum entropy and utilizes a secret key or password to generate.

Ones can copy the original CDP through P&S process and estimate the original pattern, i.e., the template. The estimation result that is printed for the second time is called a fake CDP. This process is called an estimation attack, as shown in Figure 1. Estimating the CDP pattern is one of the important tasks in the CDP image restoration task. If the restoration results give a low bit error rate (BER), then one might be able to create a fake

CDP that is hard to distinguish from the original [6]. Authentication is a process to differentiate the authentic CDPs and fake CDPs. The authentication model can be a machine learning or a statistical model. The authentication and estimation processes are depicted in Figure 1.

Deep learning (DL) has become a new technology applicable to several fields [7]–[9]. There are various usages of DL to predict hidden patterns and recover a particular signal by removing the noises [10]–[12]. This work focuses on improving the CDP estimation and authentication method in [13]. Lowering the prediction error on CDP estimation makes the CDP authentication increase the false positive. It shows the effectiveness of CDP, whether it can be copied or not. Thus, the CDP estimation attack should be mitigated with a better authentication method to detect the original and fake CPDs. In this paper, DL model is utilized, i.e., the convolutional neural network (CNN) model, to predict the CDP pattern. Compared to the previous study [13], the proposed model was able to achieve better performance in estimating the pattern of CDP.

In addition, the unsharp mask filter as an input preprocessing method used in [13] was investigated whether it could improve the model performance or not. The authentication process used a threshold score based on the estimation CDP score using the estimation model. It will accommodate the question of whether the restored CDP can be distinguished from the original CDP. Finally, the contributions of this paper are summarized as follows:

- architecture design of a CNN-based estimation model,
- comparing the effect of preprocessing of input CDP images for the developed CNN model, and
- evaluating the authentication of CDP using the estimation model.

II. CDP METHOD

Several previous studies discussed various aspects of CDP. A new metric (extracted feature) proposed in [14], the 486 feature type, to use as the quantitative value of CDP authenticity evaluation with better performance than existing metrics commonly used. In this study, the proposed metric was compared to the following metrics: (1) entropy metric, (2) Fourier domain sharpness metric, (3) wavelet domain sharpness metric, and (4) prediction error metric. The metrics included in the study were compared and evaluated on five existing restoration methods as a form of an attack on CDP: (1) Wiener filtering, (2) constrained least squares filtering, (3) Lucy-Richardson algorithm, (4) filter method, and (5) Photoshop's smart sharpen filter. These attack methods aim to improve the quality of the faked CDP to be indistinguishable from the authentic prints. Each type of attack is then evaluated with each type of feature and is compared by the error rate of each pairing. A higher error rate indicates a better performance by the attack method. Thus, it indicates lesser robustness of the metric currently evaluated.

From the evaluation of the original CDP, both wavelet and proposed 486 feature types achieved zero error rates. Evaluation on the photoshop attack had the best performance on 486 feature type achieving a lower error rate of 2.43%. Evaluation of the Sharpness (a=0.5) attack, 486 features also achieved the lowest error rate of 2.47%. Similarly, for the Sharpness (a=1) attack, the proposed 486 feature achieved the lowest error rate of 4.83%. Evaluation of the wiener filter attack is lowest on the wavelet feature with an error rate of 1.83%, whereas the 486 feature types with a higher error rate of 2.80%.

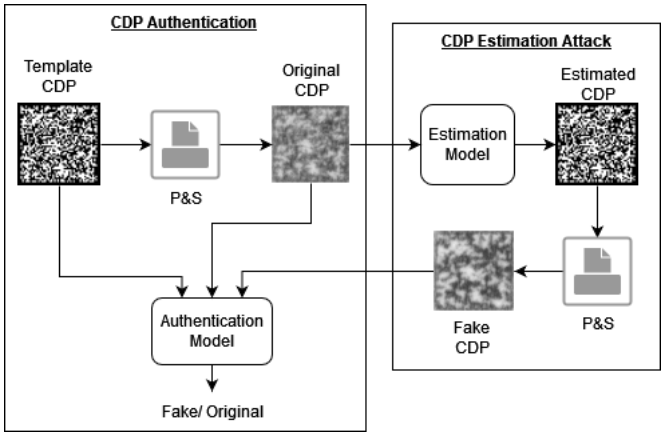

Figure 1. CDP authentication and estimation workflow.

The evaluation of the Lucy-Richardson Attack is lowest on Wavelet Feature Type with an error rate of 6.47% and 486 Feature Type achieving a lower error rate of 2.57%. Evaluation of the constrained least squares filtering attack is lowest on wavelet feature type with an error rate of 0.93% and 486 feature type achieving a higher error rate of 2.23%. The proposed 486 Feature Type achieved a lower error rate on every single attack method compared to other metrics, except on two attack methods (Wiener filtering and constrained least squares filtering).

The authors also proposed a new one-class classifier by adopting the one class classifier support vector domain description (SVDD), which is appropriate for the imbalanced class problem. The performance was evaluated with three ratios: (1) ratio of false positive to positive samples (false alarm or FR); (2) ratio of false negative to negative samples (missing alarm or FA); and (3) error rate (PE). The evaluation was done twice, using all 486 feature type generated and only using selected fourteen feature types with low error rates. When using all 486 features, the SVDD classifier achieved 16.67% in terms of FR, 6.85% in terms of FA, and 7.15% in terms of PE. When using fourteen selected features, the SVDD classifier achieved performance scores of 6.67% in terms of FR, 8.54% in terms of FA, and 8.48% in terms of PE.

Similarly, [15] employed a one class support vector machine (OC-SVM) for the authentication method. The research aimed to examine the feasibility of CDP authentication under real-world conditions, by using codes that were printed on an industrial printer and captured by a modern mobile phone. The CDP's ability to authenticate was evaluated against four different types of counterfeit copies. The findings indicate that the combination of modern machine-learning techniques and the advanced capabilities of contemporary mobile phones make it possible to authenticate CDPs even in the presence of unknown counterfeit copies. However, manual feature extraction was employed before feeding to the classifier. The performance of the classifier depends on the type of features used in the study.

Several estimation methods were compared to two other baseline methods [16]: (1) template estimation alternatives based on the LDA algorithm and (2) binarization based on Otsu's adaptive thresholding. The estimation methods were then evaluated by implementing these similarity metrics: (1) Hamming distance for binary images (HAMMING); (2) structural similarity index (SSIM); (3) Jaccard index (JACCARD); and (4) normalized cross-correlation (CORR). The performance of the estimation method was measured

p-ISSN 2301–4156 | e-ISSN 2460–5719

across a range of code density from lower to higher entropy values on a dataset generated from two different print-and-scan devices. On the highest density tested (50%) with Hamming Distance as the metric, the proposed estimation method achieved 6.17% and 7.57% probability from each print-and-scan device, lower than the two baseline methods, 18.13% and 20.01% of the Otsu method, and 15.24% and 16.34% of the LDA method. This study further evaluated the proposed method with simultaneous usage of metrics pairing in order to achieve the desired result showing a separability between the original and fakes. The pairing of HAMMING and SSIM achieved the best performance, with the lowest miss score of 5.05% and FA score of 6.88%.

CDP dataset that consists of a digital template, original P&S, and fake CDP was collected in [13]. The experiment was conducted using datasets consisting of (1) print of unique CDP (5.000 originals with its corresponding templates and 10.000 copies) and (2) print of CDP per batch (2.500 originals with its corresponding templates and 10.000 copies). BER was used as the metric to evaluate the effectiveness of an estimation attack. The smallest BER means a better estimation attack. The estimation attack "Otsu+unsharp" used a radius of 2,875 and an amount of 10. An estimation attack with a neural network approach was also conducted. The images were divided into patches of size 13 × 13 = 169. Two proposed architectures were used: (1) a fully connected neural network with 2, 3, and 4 hidden layers (FC2, FC3, FC4 respectively) with each layer size equal to input size (169); and (2) bottleneck DNN (BN DNN) model with two fully connected hidden layers of size 128 and 64 at the encoder and decoder parts and size 32 latent representation. The architecture was reimplemented from [17]. The training parameters used were 25 epochs, 128 batch size, with ReLU as its activation function, mean squared error (MSE) as its loss function, Adam [18] with a learning rate of 10^{-3} as the optimizer. The approach with the best result (lowest BER percentage) was the estimation attack using BN-DNN with a mean BER of 23.27% on unique estimation attacks and 18.47% on batch estimation attacks. Pearson correlation score was used as the metrics for the authenticity test between the template CDP and the test scanned CDP.

In this paper, the proposed model and the authentication method are evaluated using a dataset in [13], as it is available publicly and relatively new and published in 2022.

III. COPY DETECTION PATTERN

The copy detection pattern is a small dense binary pattern that is spatially sensitive on the P&S process [13]. The main idea in CDP is the information loss principle, i.e., every time the digital image is printed and scanned the quality of image always be reduced. Figure 2 illustrates the information loss principle during P&S process. It shows that the P&S process on CDP is impossible to predict perfectly because the pattern is very sensitive i.e., tiny which can be degraded due to the printer resolution and noisy which is hard to predict the pattern.

The authentication process consists of two steps. First, the digital CDP image was registered and generated using a specific pattern. This image was then printed on an item with an authorized printer. The second step is a verification process. The printed CDP was scanned with an authorized reader, then it was passed into an authentication test based on the similarity score compared to the registered image. If the test is passed, then the item is authentic or is considered as an original CDP as previously shown in Figure 1 at Section I.

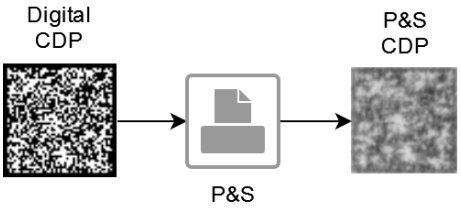

Figure 2. P&S process of CDP led to the degradation of the image quality.

The most common attack on CDP is estimating the digital template using the authentic printed CDP. The printed CDP was restored to its finest version to replicate the digital template. There are several methods used in CDP estimation attacks, such as manual restoration using image processing software, Otsu restoration, deep learning, etc.

IV. METHOD

A. DATASET

The dataset from [14] was used in the model's development process. This dataset was relatively new and consisted of 5000 unique CDPs. The dataset consisted of (1) print of unique CDP and (2) print of CDP per batch. All images in the dataset were sized at 52 × 52 pixels, with $u = 1$ pixel per elementary unit which was defined at 600 ppi (pixel per inch). These digital CDPs were printed with 600 dpi (dot per inch) and scanned with 2,400 dpi printer Canon IR-ADV C5535i, producing images sized at 208 × 208 pixels on the printed and scanned codes with a $v = 4$ pixel per elementary unit. The first dataset contains 5,000 unique original CDP images with their corresponding template 10,000 copies. The second dataset, the batch dataset, was generated with 50 unique CDP images, each printed and scanned 50 times, thus producing a database consisting of 2,500 originals with corresponding templates.

B. PROPOSED MODEL

The P&S process is a spatially sensitive process. The resulting image from each process may possess spatially related information. The proposed deep learning model will take into account the spatial dependency of the image which is achieved by implementing a convolutional neural network (CNN) architecture. CNN is a deep learning algorithm which takes an input image and then assigns importance (learnable weight and biases) to various aspects/objects in the image in order to differentiate among the images. The CNN model utilized the spatial convolution operator as a transformation method to produce a new representation of the spatial feature images. CNN model has a built-in feature extraction method; thus, manual feature extraction is not needed [19]. However, fewer preprocessing is required for the CNN algorithm, making it easier to achieve the desired result compared to other classification algorithms.

A deep learning CNN model was proposed for better performance in CDP estimation. CNN was chosen to take into account the spatially sensitive nature of the P&S process, in which 1 pixel may be affected by the surrounding pixel values. With a CNN model, the needed local information is preserved, CNN algorithm reduces an image into another form that is easier to process without losing the important features and information from the original image. The proposed model, CDP-CNN, has three main blocks, i.e., residual, concatenation, and gating blocks, as shown in Figure 3. The gating block utilizes 1 × 1 convolution, in which each channel has its own

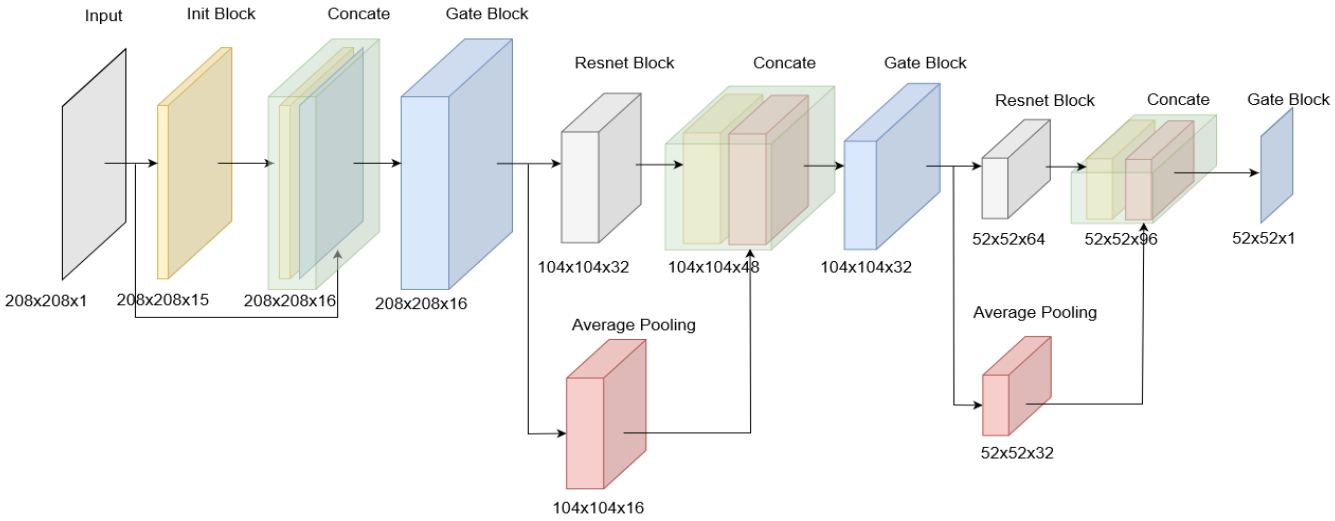

Figure 3. CDP-CNN model architecture.

TABLE I
PERFORMANCE OF UNIQUE ESTIMATION ATTACK

Method	BER	STD	Max	Min
BN-DNN [13]	23.27%	-	26.99%	20.31%
*CDP-CNN	17.46%	1.01%	20.97%	14.09%
*CDP-CNN + unsharp_mask	17.39%	1.01%	21.01%	14.05%
*t-stats=-47.37, pvalue=0.00				

TABLE II
PERFORMANCE OF BATCH ESTIMATION ATTACK

Unique CDP	BER	STD	Max	Min
BN-DNN + unsharp_mask [13]	25.27%	0.72%	-	-
*CDP-CNN	19.64%	1.50%	26.78%	15.24%
*CDP-CNN + unsharp_mask	19.47%	1.53%	27.00%	15.20%
*t-stats=-37.36, pvalue=0.00				
Batch CDP	**BER**	**STD**	**Max**	**Min**
BN-DNN [14]	18.47%	0.72%	-	-
*CDP-CNN	10.36%	0.49%	11.43%	9.02%
*CDP-CNN + unsharp_mask	9.91%	0.62%	11.50%	8.51%
*t-stats=-0.83, p-value=0.2				

characteristics. The gating method was implemented to act as an ensemble mechanism for each pixel, as the input of this block is the concatenation of residual and previous gating blocks. The CDP-CNN model also utilizes the skip connection found in ResNet models [20]. The skip connection allows the gradient to be transported much easier into the earlier layer of the model to enhance the learning process facilitated on residual blocks.

The last layer of the model has a spatial dimension of 52 × 52 × 1, which matches the ground truth or the template. The last layer was passed to the binary cross-entropy loss function as the task is a pixel-wise binary classification problem.

Compared to the bottleneck (BN) model used in [13], the CDP-CNN model has fewer parameters, i.e., 50.2 thousand parameters, whereas the BN model has 64.8 thousand parameters.

C. EXPERIMENTAL SETUP

The dataset was split using the same procedure as in [14], i.e., with 2,500 train images, 1,000 validation images, and 1,500 test images. The training was done with 50 epochs and utilizing the auto-finder to find the best learning rate for the model using Pytorch library [21]. Adam was used as the optimizer [18]. The model will first learn from the training images to then make predictions on the validation dataset. The best model that will be chosen was determined from the model performance on the validation data. The best model was evaluated on the testing dataset to obtain the final accuracy of the proposed model. All code implementations are available online in our repository.

D. STATISTICAL TESTING

In this paper, the performance of a model with an unsharp and a model without an unmask filter were compared. The one tailed t-test was used to investigate whether the difference of the model's performance was significant. A margin difference of 0.5% was used with a p-value threshold, α of 1%. The sample used in this statistical testing was the paired BER difference between the model with and without the unsharp filter, i.e, $diff = BER_{withoutUnsharp} - BER_{withUnsharp}$.

The null hypothesis, H_0, is the performance difference not less or equal to 0.5%. Whereas the alternative hypothesis, H_1, is the performance difference less than 0.5%. If the p-value is less than the given threshold of 1%, then the H_0 is rejected, otherwise H_0 cannot be rejected.

V. EXPERIMENTAL RESULT

In this section, the proposed models are evaluated. The models were trained in the same dataset with different input preprocessing. Two DL-based models are a model with unsharp mask input and a model without unsharp mask input. The unsharp mask filter was discussed in [13].

A. CDP ESTIMATION PROCESS

The printed CDP patterns are estimated using the proposed model, CDP-CNN. From Table I, the BER was 17.46% for the model without the unsharp mask and 17.39% for the model with the unsharp mask filter. These values are better than the current performance shown in [13], i.e., 23.27%. Both model's performances show the statistical difference with a p-value less than 0.01, meaning that the difference between the two models is significantly less than 0.5%, i.e., the null hypothesis is

p-ISSN 2301–4156 | e-ISSN 2460–5719

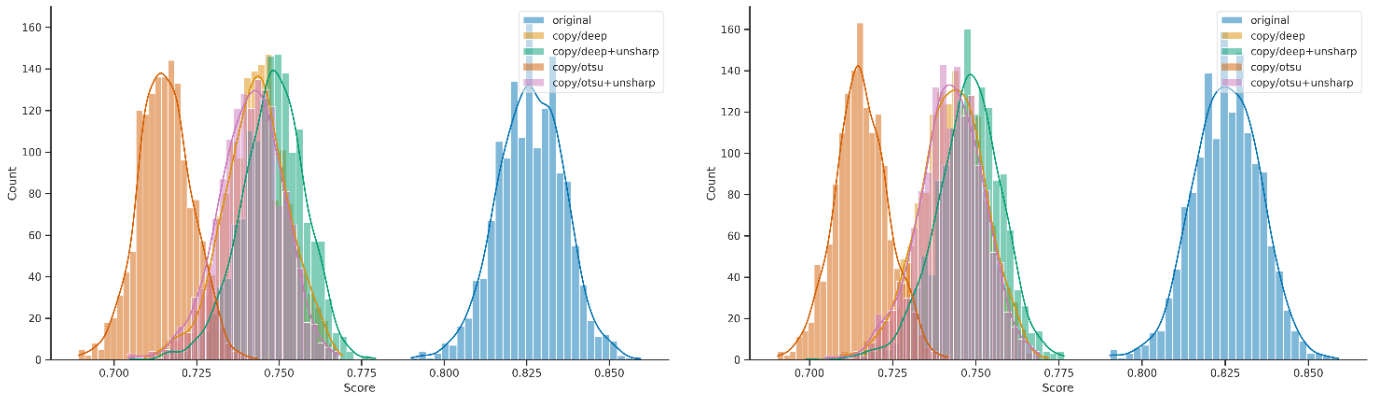

Figure 4. Authentication process using (a) estimation model with unsharp mask (b) estimation model without unsharp mask. Both models show a good separation between the fake and original distribution.

rejected. Thus, the effect of using a preprocessing filter, unsharp mask, in estimating the original CDP using CDP-CNN model did not significantly improve the model's performance. Similarly, the models were applied to batch CDP datasets, both on individual (unique CDP) and batch CDP estimation schemes.

In individual or unique CDP on batch datasets, the result also shows that the difference between the model with and without the unsharp mask filter is significantly less than 0.5%. On the other hand, the model with an unsharp mask performed better than the model without an unsharp mask filter on batch CDP estimation, with a p-value of 0.2, i.e., the null hypothesis is accepted, as shown in Table II. In this case, the model with an unsharp mask filter applied to the input image is significantly better than the model without the unsharp mask based on the statistical testing, with a relative difference of not less or equal to 0.5%. Therefore, the model with an unsharp mask tends to help estimate CDP patterns with the batch scheme.

Moreover, all results in this experiment provided much better BER than the previously reported result in [13], as shown in Tables I and II. The CDP-CNN model was 5% better than [13] on unique estimation attacks and 9% better on batch estimation attacks.

The model used in this study was CNN based model, while the previous model used multi-layer perceptron (MLP) architecture, i.e., autoencoder structure. Generally, the CNN model shows better performance than MLP in the case of image processing tasks, such as predicting the CDP pattern [22]. Moreover, the CDP-CNN model utilized fewer parameters than the autoencoder model used in [13], precisely 21% fewer parameters.

B. CDP AUTHENTICATION PROCESS

There are four sources of fake CDP datasets from [13], i.e., deep (BN model), deep+unsharp, Otsu, and Otsu+unsharp. The Otsu dataset was obtained from the scanned original CDPs estimated using the Otsu method; then the estimated CDPs were printed and scanned. The same mechanism was also applied to generate the other datasets for different methods. However, the authentication process used in this paper is an estimation score from the model used in CDP estimation models. The scanned CDP images were passed to the estimation model. The score was calculated using the total bit accuracy score, i.e., 1- BER. The mean, μ, and standard deviation, σ, of the distribution of original CDPs were calculated to define the threshold parameter, $\epsilon = \mu - 4\sigma$, to distinguish between original and fake CDPs. Figure 4 shows the separation of the original and the fake CDPs produced by the attack methods. Both models, i.e., the model with and without unsharp filters, show good separation distribution. There is no false positive and false negative on detecting the original CDPs, using $\epsilon = \mu - 4\sigma$. Thus, the estimation model is also reliable to use for the authentication methods in determining the original or fake CDPs.

C. DISCUSSION

From the results in the previous section, the BER of the best model is around 10%, which is still impossible to make the BER zero. Thus, CDP estimation is still a secure method for anti-counterfeiting products. Moreover, the trained CDP-CNN model contains information about the quality of the CDP image from the training process, making it suitable to use as an authentication method. Additionally, the CNN-based model is more straightforward to implement than manual feature extraction with a particular classifier.

However, there are limitations to the proposed method. The method was only tested on specific types of devices (a single printer and scanner), and it may not perform well on other devices. Therefore, it would be important to test the model on multiple devices to ensure its effectiveness in real-world scenarios, since in production, the devices used by the end users cannot be controlled.

VI. CONCLUSION

A state-of-the-art CDP estimation model based on CNN architecture was proposed. The proposed model effectively performs better on the same dataset used by the previous study, with a better accuracy metric (smaller BER) and a more efficient training process with less count of parameters. The utilization of CNN architecture also exempts the need to implement unsharp masking that is proven to be insignificant with one-tailed t-statistical testing. However, the unsharp mask filter significantly reduced the BER by at least 0.5% on batch estimation attacks. The CDP-CNN estimation model was 5% better than the previous state-of-the-art model on unique estimation attacks and 9% better on batch estimation attacks. Moreover, the authentication method used the score from the estimation model, which had an excellent separation to distinguish between original and fake CDP. Thus, one model can be used for both tasks. The BER of the proposed model was

9.91% on batch CDP estimation. It might increase the false positives of the authentication process. However, in the future, an ad-hoc DL-based authentication model might be required to further improve the separation of the distribution between fake and original CDPs.

CONFLICT OF INTEREST

The authors declare that the article entitled "CNN-Based Model for Copy Detection Pattern Estimation and Authentication" has no conflict of interest.

ACKNOWLEDGMENT

The authors would thank Yusuf Helmy Hensyaputra for assistance in revising this article and monitoring the experimental result.

AUTHOR CONTRIBUTION

Conceptualization, Syukron Abu Ishaq Alfarozi and Azkario Rizky Pratama; methodology, Syukron Abu Ishaq Alfarozi; experiment and simulation, Syukron Abu Ishaq Alfarozi; validation, Syukron Abu Ishaq Alfarozi and Azkario Rizky Pratama; formal analysis, Syukron Abu Ishaq Alfarozi and Azkario Rizky Pratama; investigation, Syukron Abu Ishaq Alfarozi and Azkario Rizky Pratama; resources, Syukron Abu Ishaq Alfarozi; data curation, Syukron Abu Ishaq Alfarozi; writing—original draft preparation, Syukron Abu Ishaq Alfarozi; writing—review and editing, Syukron Abu Ishaq Alfarozi and Azkario Rizky Pratama;

REFERENCES

[1] E. Gasiorowski-Denis (2014) "Crackdown on counterfeiting," [Online], https://www.iso.org/news/2014/01/Ref1809.html, access date: 26-Jul-2022.

[2] L. Korsell, "Fraud in the Twenty-First Century," *Eur. J. Crim. Policy Res.*, Vol. 26, No. 3, pp. 285–291, Aug. 2020, doi: 10.1007/s10610-020-09463-2.

[3] OEICD/EUIPO (2016) "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact," [Online], https://read.oecd-ilibrary.org/governance/trade-in-counterfeit-and-pirated-goods_9789264252653-en#page5, access date: 26-Jul-2022.

[4] A. Anderson (2006) "Combating Counterfeiting: Simple Steps You Can Take Now to Protect Your Brand from Piracy," [Online], https://www.hollandhart.com/articles/CounterfeitingArticleAndersonRev2.pdf, access date: 26-Jul-2022.

[5] J. Picard, "Digital Authentication with Copy-Detection Patterns," *Proc. Vol. 5310 Opt. Secur. Counterfeit Deterrence Tech. V, R.L. van Renesse, Ed.*, Jun. 2004, pp. 176–183, doi: 10.1117/12.528055.

[6] C. Chen *et al.*, "A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models," *IEEE Trans. Inf. Forensics, Secur.*, Vol. 15, pp. 1056–1071, Aug. 2019, doi: 10.1109/TIFS.2019.2934861.

[7] I.H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Comput. Sci.*, Vol. 2, No. 6, pp. 1–20, Nov. 2021, doi: 10.1007/s42979-021-00815-1.

[8] P.R. Kumar and E.B.K. Manash, "Deep Learning: A Branch of Machine Learning," *J. Phys. Conf. Ser.*, Vol. 1228, pp. 1–9, May 2019, doi: 10.1088/1742-6596/1228/1/012045.

[9] K. Choudhary *et al.*, "Recent Advances and Applications of Deep Learning Methods in Materials Science," *npj Comput. Mater.*, Vol. 8, pp. Apr. 2022, doi: 10.1038/s41524-022-00734-6.

[10] V. Kober, T. Choi, V. Diaz-Ramírez, and P. Aguilar-González, "Pattern Recognition: Recent Advances and Applications," *Math. Probl. Eng.*, Vol. 2018, pp. 1–2, 2018, doi: 10.1155/2018/8510319.

[11] B. Liu and J. Liu, "Overview of Image Denoising Based on Deep Learning," *J. Phys. Conf. Ser.*, Vol. 1176, No. 2, pp. 1–6, Mar. 2019, doi: 10.1088/1742-6596/1176/2/022010.

[12] K. Yun, A. Huyen, and T. Lu, "Deep Neural Networks for Pattern Recognition," 2018, *arXiv:1809.09645*.

[13] E. Khermaza, I. Tkachenko, and J. Picard, "Can Copy Detection Patterns be Copied? Evaluating the Performance of Attacks and Highlighting the Role of the Detector," *2021 IEEE Int. Workshop Inf. Forensics, Secur. (WIFS)*, 2021, pp. 1–6, doi: 10.1109/WIFS53200.2021.9648384.

[14] P. Zhang, W. Zhang, and N. Yu, "Copy Detection Pattern-Based Authentication for Printed Documents with Multi-Dimensional Features," *2019 7th Int. Conf. Infor. Commun., Netw. (ICICN)*, 2019, pp. 150–157, doi: 10.1109/ICICN.2019.8834939.

[15] O. Taran *et al.*,"Mobile Authentication of Copy Detection Patterns: How Critical Is to Know Fakes?" *2021 IEEE Int. Workshop Inf. Forensics, Secur. (WIFS)*, 2021, pp. 1–6, doi: 10.1109/WIFS53200.2021.9648398.

[16] R. Chaban *et al.*, "Machine Learning Attack on Copy Detection Patterns: Are 1 × 1 Patterns Cloneable?" *2021 IEEE Int. Workshop Inf. Forensics, Secur. (WIFS)*, 2021, pp. 1–6, doi: 10.1109/WIFS53200.2021.9648387.

[17] O. Taran, S. Bonev, and S. Voloshynovskiy, "Clonability of Anti-counterfeiting Printable Graphical Codes: A Machine Learning Approach," *ICASSP 2019 - 2019 IEEE Int. Conf. Acoust. Speech, Signal Process. (ICASSP)*, 2019, pp. 2482–2486, doi: 10.1109/ICASSP.2019.8682967.

[18] D.P. Kingma and J.L. Ba, "Adam: A Method for Stochastic Optimization," 2017, *arXiv:1412.6980v9*.

[19] S. Saidah, I.P.Y.N. Suparta, and E. Suhartono, "Modifikasi Convolutional Neural Network Arsitektur GoogLeNet dengan Dull Razor Filtering untuk Klasifikasi Kanker Kulit," *J. Nas. Tek. Elekt., Teknol. Inf.*, Vol. 11, No. 2, pp. 148–153, May 2022, doi: 10.22146/jnteti.v11i2.2739.

[20] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," *2016 IEEE Conf. Comput. Vis., Pattern Recognit.*, 2016, pp. 770–778, 2016, doi: 10.1109/CVPR.2016.90.

[21] A. Paszke *et al.*, "PyTorch: An Imperative Style, High-Performance Deep Learning Library," in *NIPS,19: Proceedings of the 33rd International Conference on Neural Information Processing Systems*, H.M. Wallach *et al.*, Eds., Red Hook, NY, USA: Curran Associates Inc., 2019, pp. 8026–8037.

[22] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-Based Learning Applied to Document Recognition," *Proc. IEEE*, Vol. 86, No. 11, pp. 2278–23234, Nov. 1998, doi: 10.1109/5.726791.