Detecting Copy-Move Forgery in Images Using Convolutional Neural Networks (CNNs)

Alaa Bashir Zabiya[1], Fatima Baio Madi[1], Mustafa Ali Abuzaraida[1]

[1] Misurata University, Misurata, Libya.

***Abstract*— Recently, digital images have become widely used in various fields, attracting the attention of researchers in the field of digital image processing. This research focuses on detecting a type of image forgery using Convolutional Neural Networks (CNN), specifically the copy-move forgery. In this forgery, a portion of the image is copied and pasted onto another part of the same image. The research proposes a CNN-based network structure for detecting copy-move forgery in images. The model is trained on different datasets previously used in this domain and then tested on a new dataset to reliably evaluate the efficiency of the proposed model. The model was trained on the (MICC-F2000) dataset and achieved an accuracy of up to 97.75%. It was also trained on the (CoMoFoD) dataset and achieved an accuracy of up to 92.85%. The results of testing the trained models on the new dataset indicate the superiority of the model trained on the (MICC-F2000) dataset. However, both models did not achieve high accuracy due to the fact that the forgery in the new dataset is unclear and difficult to detect with the naked eye.**

***Index Terms*—digital images, image forgery detection, copy-move, deep learning, convolutional neural network (CNN).**

I. INTRODUCTION

In recent years, the use of digital images has become widespread due to advancements in technology. They are now used in various fields, including law [1], forensic medicine [2], and social media. Images are preferred over text as they convey information more clearly. However, this popularity has also led to an increase in image manipulation. While some modifications, like adjusting brightness and contrast, are harmless and improve image quality. others can be harmful, these modifications compromise the integrity of the image and can cause harm to others. With the availability of powerful image editing tools, it has become easier to forge images, leading to concerns about their authenticity. Image forgery has been defined as the process of manipulating a digital image to hide its original identity or to create a completely different image from what was intended, and copy-move forgery is one of the most used forgery techniques where a part of the image is copied and pasted on another part of the image, this technique can be harmful if used by someone with malicious intent; therefore, it is necessary to raise awareness that not all images are trustworthy and to develop methods for detecting image forgery and identifying the area of manipulation [3]. Where image forgery detection refers to image authentication and detection of the part that has been tampered within the image, which is done by calculating the statistical characteristics of each section of the image and comparing them with each other [4]. There are two ways to verify the authenticity of digital images, the active approach and the passive approach, as shown in Figure 1. The active approach involves embedding a security structure, such as a digital signature or watermark, within the image during its creation. The image signature is then extracted and compared to the original signature. If the extracted signature matches the original signature, the image is considered authentic; otherwise, it is classified as a forgery. While the passive approach analyzes the contents and structure of an image to verify its validity and credibility without embedding a signature or watermark [5]. Various techniques are employed under the passive approach to detect copy-move forgeries. These techniques include block generation techniques and keypoint-based techniques. Their primary focus is to enhance the detection rate and ensure robustness against image transformations such as fog, scaling, and rotation. The process of detecting copy-move forgery includes several main steps. First, feature extraction is performed. Then, similarity is verified by linking matching parts together. Finally, the image is classified as either original or forged. PCA and DCT are examples of block generation techniques used for detecting copy-move forgery, while there are a number of keypoint-based techniques such as: SIFT and SURF [6].

DOI:http://doi.org/10.24086/cocos2024/paper.1170

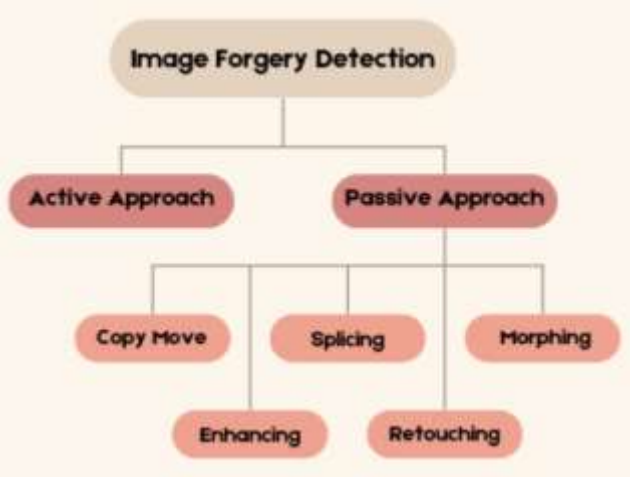

Figure 1. Types of digital image forgery detection.

Types of image forgery:

There are several types of digital image forgery, and these types vary depending on how image processing techniques are employed to manipulate and alter information within the images. The first type of digital image forgery is known as copy-move forgery, in which a part of the image is copied and pasted into another location within the same image, as shown in Figure 2. The second type is splicing forgery, where two or more images are merged into a single image to create a forged image, as shown in Figure 3. The third type refers to image morphing, which is a smooth animated transition from one image to another, where one object is transformed into another in the process, as illustrated in Figure 4. The fourth type is image retouching, which is enhancing selective parts of the image, reducing specific features, and improving its overall quality to capture the attention of viewers, this type is often used in portrait photography or fashion industry as shown in Figure 5. The final type is image enhancement, where the brightness, contrast, color balance and sharpness of the image are adjusted to make it look better, as shown in Figure 6 [5].

Figure 2. copy-move forgery.

Figure 3. splicing forgery.

Figure 4. image morphing**.**

Figure 5. image retouching**.**

Figure 6. image enhancement.

Convolutional Neural Networks (CNNs):

Convolutional Neural Networks (CNNs) are a type of artificial neural network designed to mimic the communication structure between nerve cells in the human brain [8]. They are among the most popular deep learning algorithms. CNNs employ a series of overlapping neural convolutional layers to progressively analyze an image and extract relevant information from specific regions. They consist of three main layers: the convolutional layer, the pooling layer, and the fully connected layer, with each layer serving a distinct role [9]. These layers are shown in Figure 7. CNNs have demonstrated its effectiveness in various fields, showcasing remarkable success in tasks such as image classification, object detection, natural language processing and other domains [10]. Consequently, CNNs form an essential part of many fields that rely on deep learning [8].

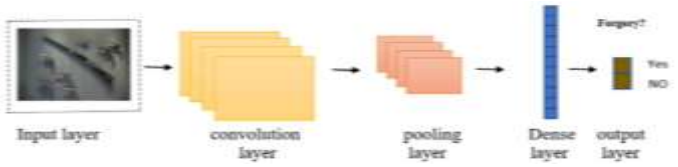

Figure 7. The main layers of CNN [11].

DOI:http://doi.org/10.24086/cocos2024/paper.1170

Convolutional Layer: This layer is responsible for extracting various features of an image, such as edges, corners, and key points. The convolutional layer operates by sequentially applying the convolution process to the input image at all possible locations, utilizing a set of diverse filters or kernels to generate a feature map, as shown in Figure 8.

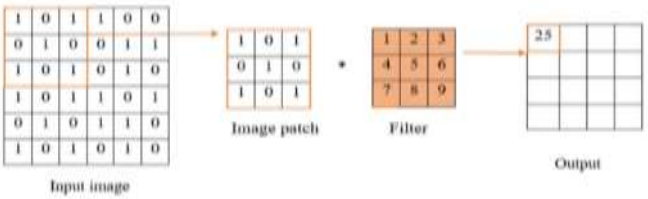

Figure 8. Convolutional Layer [11].

Pooling Layer: The pooling layer is responsible for reducing the spatial dimensions of the feature maps generated by the convolutional layer. This limits the number of parameters in the convolutional neural network and prevents overfitting. Additionally, the pooling layer enhances the network performance and the quality of features extracted from the image. There are several types of pooling layers, each differing in the method of value selection and the size of the selection region. The most common type is the max pooling layer, which extracts the most important features from the image, as shown in Figure 9.

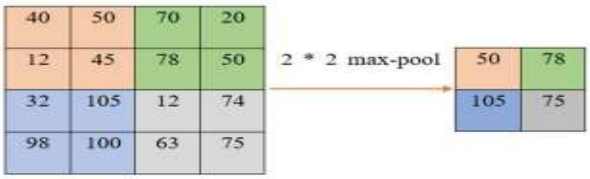

Figure 9. max pooling layer [11].

Fully Connected Layer: This layer is responsible for the final classification, consisting of a set of interconnected nodes (neurons). The fully connected layer receives signals from the preceding layers in the neural network and transforms them into output signals, which represent the final result of the neural network. In addition to these layers, convolutional neural networks may include other types of layers depending on the specific application and network structure, such as:

• **Flatten layer:** It is commonly used between deep neural layers and fully connected layers to convert data from a multidimensional shape (2D or 3D) to a single vector shape (1D). This transformation enables the fully connected layers to effectively process the data.

II. Related Works

The related works in this paper primarily focus on investigating copy-move forgery. Parveen et al. [12] proposed a method for detecting copy-move image forgery using discrete cosine transform (DCT) and K-means. Narayanan et al. [13] proposed a copy-move forgery detection technique that combines keypoint detection methods and block-based methods. Hilal et al. [14] proposed a combination of principal component analysis (PCA) and DCT to identify copy-move image forgery. Aslam et al. [15] used the DCT and deep learning approach to learn features for detecting manipulated images. Mahdi et al. [16] utilized the SIFT technique to extract features and the wavelet technique to estimate the matching threshold. Ashraf et al. [17] proposed a technique designed on the basis of overlapping square blocks to detect copy-move forgery (CMIF) in digital images using discrete wavelet transform (DWT). Dhivya et al. [18] proposed a copy-move forgery detection technique that utilizes the SURF feature extraction technique, and a supervised learning technique called Support Vector Machine (SVM). Rathore et al. [19] proposed a copy-move forgery detection algorithm based on IRVM, which uses biorthogonal wavelet transform (BWT) with singular value decomposition (SVD) to efficiently extract and classify features. Muniappan et al. [20] presented a methodology for detecting copy-move forgery based on a deep learning approach using a CNN model.

III. 3.Proposed Method

The CNN structure In this research, a model utilizing CNN was developed for the detection of copy-move forgery in images, as illustrated in Figure 10. The methodology comprises three stages: preprocessing, feature extraction, and classification. In the preprocessing stage, the input image size was adjusted to (224×224) without any cropping, and the image was converted to grayscale. Next, in the feature extraction stage, features were extracted from the images using the first three blocks shown in Figure 10. Each block consists of a convolutional layer, followed by a max pooling layer, with an activation layer (ReLU) in between.The convolutional layer sequentially applies the convolution process to the input image, generating feature maps using its set of filters. The activation layer (ReLU) receives these feature maps and converts negative signals to zero while leaving positive signals unchanged. Subsequently, the max pooling layer reduces the spatial dimensions of the feature maps produced by the convolutional layer and selects the

DOI:http://doi.org/10.24086/cocos2024/paper.1170

maximum value from each feature map. This process enhances the performance of the convolutional neural network model and improves the quality of the extracted features from the image. This sequence repeats in all blocks until the final feature maps are obtained. These maps are then passed to the flatten layer, which converts them from matrices to vectors, so that they can be used effectively by the fully connected layer. Finally, the fully connected layer connects all the extracted features from the feature extraction stage to the dense layer, which consequently yields the final result of the neural network by classifying the image as original or forged.

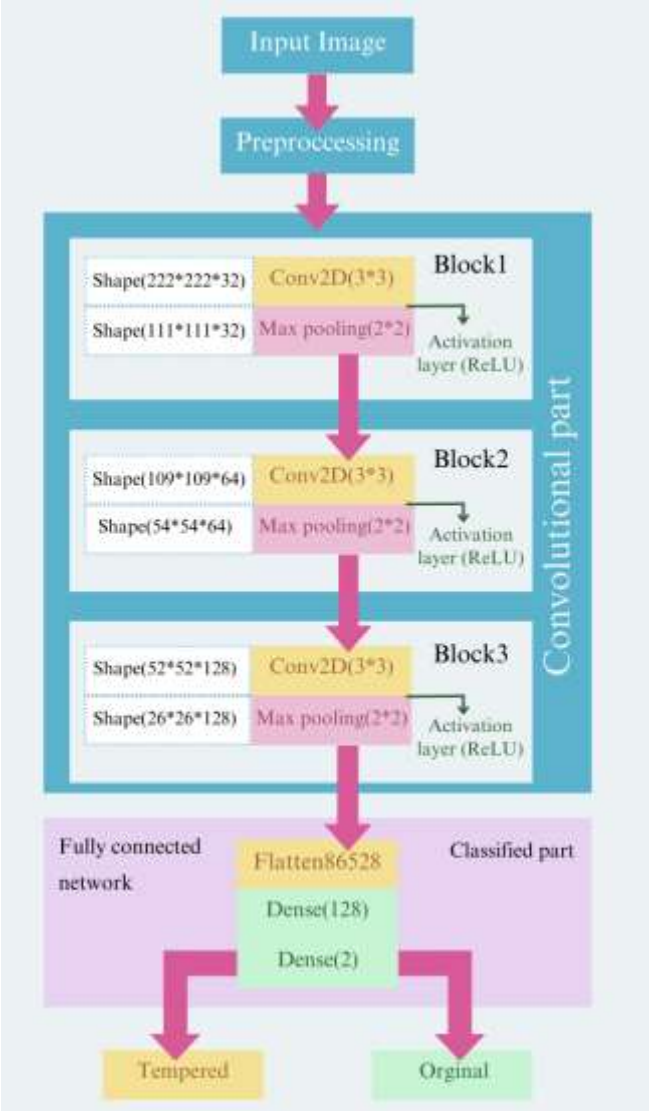

Figure 10. Structure of CNN model.

The proposed model was trained using two optimizers, namely Adam and RMSprop, with a batch size of 32. The model was trained for 35 and 25 epochs, with a learning rate of 1e-4. The primary function of the optimizers is to enhance the training process by minimizing the difference between the expected results of the model and the actual results, aiming to achieve the best model that provides accurate results.

IV. Results and Discussion

A. Datasets

In this study, three datasets were utilized to evaluate the proposed CNN model, as outlined in Table 1. Each dataset has distinct characteristics. Two of them, the MICC-F2000 [21] and the CoMoFoD [22] were publicly available and commonly employed for detecting copy-move forgery in images. Additionally, a new dataset was developed specifically to test the CNN model trained using the aforementioned datasets. In the new dataset, each image was manually forged using the Copy-move technique via the Picsart application. The forgery in this dataset involved not only the duplication of a part within the same image but also the concealment of parts by copying another part from the same image. As a result, the forged images exhibited a professional level of manipulation, presenting a significant challenge for detection and making it difficult to verify their originality. Figure 11 provides an example of the new dataset.

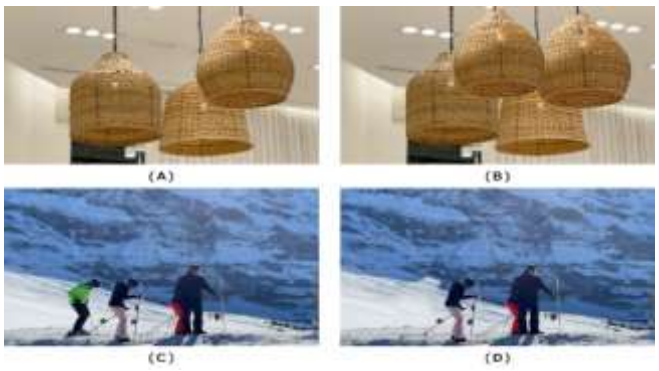

Figure 11. Example of the new dataset. Images A and C are authentic and Images B and D are fake.

DOI:http://doi.org/10.24086/cocos2024/paper.1170

Table 1. Details of the MICC-F2000, CoMoFoD, and New datasets.

Dataset	Composition				Size of image	No. of training Images	No. of testing Images	The input shape
MICC-F2000	2000 images				2048 x 1536 pixels	1600 images	400 images	224 x 224 x 3 pixels
	tampered	700	original	1300				
CoMoFoD	2800 images				512 x 512 pixels	2240 images	560 images	224 x 224 x 3 pixels
	tampered	1400	original	1400				
New data set	500 images				2048 x 1536 pixels	----------	500 images	224 x 224 x 3 pixels
	tampered	250	original	250				

B. Evaluation metrics

To estimate the accuracy of the proposed approach, evaluation metrics were used to ensure the reliability of the results according to equation number 1.

$$1.\quad \text{Accuracy} = \frac{(TN + TP)}{(TP + FP + TN + FN)} \times 100$$

Where:

• TP -True Positive represents the number of images that were correctly
classified as forged, and are expected to be forged.
• TN -True Negative represents the number of images that were correctly
classified as original and are expected to be original.
• FP -False Positive represents the number of images that were incorrectly
classified as forged, and are expected to be original.
• FN -False Negative represents the number of images that were incorrectly
classified as original, and are expected to be forged.

$$2.\quad \text{Precision} = \frac{TP}{TP + FP} \times 100$$

$$3.\quad \text{Recall} = \frac{TP}{TP + FN} \times 100$$

$$4.\quad \text{F1-Score} = \frac{2 * (\text{Precision} * \text{Recall})}{(\text{Precision} + \text{Recall})} \times 100$$

We also used the logarithmic loss (Log Loss) to identify the misclassified images. Supposing we have M classes containing N samples, the logarithmic loss is:

$$5.\quad \text{logless} = \frac{-1}{N} \sum_{a=1}^{N} \sum_{b=1}^{M} Zab.\log(Pab)$$

where Zab indicates whether (a) belongs to class (b) or not, Pab indicates that this sample (a) may belong to class (b). The accuracy value is higher if the logarithmic loss is close to zero.

C. Results

Table 2 presents the results obtained from testing the proposed CNN approach mentioned earlier, which was trained using publicly available datasets. The table showcases the performance of the trained models on these datasets On the other hand, Table 3 shows the results of testing the models on the new dataset. The objective of this evaluation is to assess the effectiveness of the proposed CNN structure in detecting forged images.

Table 2. Results for MICC-F2000 and CoMoFoD datasets.

Dataset	Epochs	Optimizer	Accuracy	Loss	Precision	Recall	F1-Score
MICC-F2000	25	RMSprop	97.75	0.0600	1.0000	0.9661	0.9825
		Adam	95.24	0.0926	1.0000	0.9283	0.9621
	35	RMSprop	97.50	0.0690	1.0000	0.9628	0.9807
		Adam	96.74	0.0734	1.0000	0.9510	0.9742
CoMoFoD	25	RMSprop	88.92	0.2327	0.9434	0.8221	0.8758
		Adam	88.57	0.2872	0.9233	0.8414	0.8744
	35	RMSprop	92.67	0.1770	0.9803	0.8711	0.9200
		Adam	92.85	0.1729	0.9716	0.8804	0.9217

Based on the preceding results table, it is evident that satisfactory outcomes were achieved overall. Notably, the MICC-F2000 dataset achieved the highest performance. The model trained with the RMSprop optimizer over 25 iterations attained the highest overall accuracy of 97.75%. Additionally, the model trained with the RMSprop optimizer over 35 iterations achieved a closely competitive accuracy of 97.50%.

DOI:http://doi.org/10.24086/cocos2024/paper.1170

ole 3. Testing models on the new dataset.

Model	Epochs	Optimizer	Accuracy	Loss
MICC-F2000	25	RMSprop	62.65	1.2844
		Adam	62.91	1.4472
	35	RMSprop	61.89	1.1569
		Adam	62.40	1.0955
CoMoFoD	25	RMSprop	46.29	3.1163
		Adam	46.03	3.9853
	35	RMSprop	41.94	4.4433
		Adam	44.24	3.4619

After testing the models on the new dataset to ensure reliable assessments Table 3 clearly indicates that the models trained on the MICC-F2000 dataset outperformed those trained on the CoMoFoD dataset.

V. Conclusion

The experimental findings presented in Table 2 demonstrate the superiority of the CNN model trained on the MICC-F2000 dataset compared to the model trained on the CoMoFoD dataset. This can be attributed to the fact that the utilized CNN structure was better suited to the characteristics of the MICC-F2000 dataset, including its size, distribution, diversity, and complexity. In contrast, the CoMoFoD dataset posed challenges such as noise, which adversely affected the model's performance. Furthermore, upon testing the models on the new dataset, the results displayed in Table 3 further confirm the superiority of the CNN model trained on the MICC-F2000 dataset over the model trained on the CoMoFoD dataset. However, it is important to note that neither model achieved high accuracy due to the unclear and challenging nature of the forgery in the new dataset, making it difficult to detect even for human observers.

References

[1] M. M. Eltoukhy, M. Elhoseny, K. M. Hosny, and A. K. Singh, ''Computer aided detection of mammographic mass using exact Gaussian–Hermite moments,'' J. Ambient Intell. Humanized Comput., pp. 1–9, Jun. 2018, doi: 10.1007/s12652-018-0905-1.

[2] A. Ross, S. Banerjee, and A. Chowdhury,''Security in smart cities: A brief review of digital forensic schemes for biometric data,''Pattern Recognit. Lett., vol. 138, pp.346354.

[3] Alzamil, Lubna. "Image Forgery Detection with Machine Learning." (2020).

[4] Sadeghi, Somayeh, et al. "State of the art in passive digital image forgery detection: copy-move image forgery." *Pattern Analysis and Applications* 21(2018): 291306.

[5] Abidin, Arfa Binti Zainal, et al. "Copy-move image forgery detection using deep learning methods: a review." *2019 6th international conference on research and innovation in information systems (ICRIIS)*. IEEE, 2019.

[6] Ega, Jahnavi, Deepak Sri Sai Krishna, and V. M. Manikandan. "A Review on Digital Image Forgery Detection." *International Journal of Engineering Research and Technology* 14.5 (2021): 419-423.

[7] Thakur, R., & Rohilla, R. (n.d.). A brief overview of recent developments in techniques for detecting digital image manipulation.

[8] M. A. Abuzaraida and O. M. Elrajubi, "Laser marks classification for retinal images based on convolutional neural network" Int. J. Eng. Adv. Technol., vol. 8, no. 6 Special Issue 3, pp. 188–193, 2019, doi: 10.35940/ijeat.F1030.0986S319.

[9] Abuzaraida, Mustafa Ali, and Osama Mohamed Elrajubi. "Improving laser mark detection for retinal images based on the AlexNet model." International Journal 9.4 (2020).

[10] Hosny, Khalid M., et al. "An efficient CNN model to detect copy-move image forgery." *IEEE Access* 10 (2022): 48622-48632.

[11] Şengöz, Nilgün, et al. "Importance of Preprocessing in Histopathology Image Classification Using Deep Convolutional Neural Network." *Advances in Artificial Intelligence Research* 2.1 (2022): 1-6.

[12] Parveen, A., Khan, Z. H., & Ahmad, S. N. (2019). *Block-based copy–move image forgery detection using DCT. Iran Journal of Computer Science.*

[13] Narayanan, Shibu S., and G. Gopakumar. "Recursive block based keypoint matching for copy move image forgery detection." *2020 11th International conference on computing, communication and networking technologies (ICCCNT)*. IEEE, 2020.

[14] Hilal, Alaa, Taghreed Hamzeh, and Samer Chantaf. "Copy-move forgery detection using principal component analysis and discrete cosine transform." *2017 Sensors Networks Smart and Emerging Technologies (SENSET)*. IEEE, 2017.

DOI:http://doi.org/10.24086/cocos2024/paper.1170

[15] Aslam, Alvina, et al. "Image Forgery Detection Using Convolutional Neural Network." (2020).

[16] Mahdi, Muthana S., and Saad N. Alsaad. "Detection of Copy-Move Forgery in Digital Image Based on SIFT Features and Automatic Matching Thresholds." *Applied Computing to Support Industry: Innovation and Technology: First International Conference, ACRIT 2019, Ramadi, Iraq, September 15–16, 2019, Revised Selected Papers 1*. Springer International Publishing, 2020.

[17] Ashraf, Rehan, et al. "An efficient forensic approach for copy-move forgery detection via discrete wavelet transform." *2020 International Conference on Cyber Warfare and Security (ICCWS)*. IEEE, 2020.

[18] Dhivya, S., J. Sangeetha, and B. J. S. C. Sudhakar. "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique." *Soft Computing* 24 (2020): 14429-14440.

[19] Rathore, Neeraj Kumar, et al. "Image forgery detection using singular value decomposition with some attacks." *National Academy Science Letters* 44 (2021): 331-338.

[20] Muniappan, Thiiban, et al. "An Evaluation of Convolutional Neural Network (CNN) Model for Copy-Move and Splicing Forgery Detection." *International Journal of Intelligent Systems and Applications in Engineering* 11.2 (2023): 730-740.

[21] Copy-Move Forgery Detection and Localization | Image and Communication Laboratory (unifi.it)

[22] COMOFOD | Kaggle

[23] O. M. Elrajubi, M. A. Abuzaraida, and A. M. Zeki, "Retinal image laser marks detection using a convolutional neural network" in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2018, 2018, pp. 1–5, doi: 10.1109/3ICT.2018.8855784.

DOI:http://doi.org/10.24086/cocos2024/paper.1170