Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Multilayer Perceptron Network to Detect Fraud in Digital Images

Omnea Alkhoja[1, *]

[1] Islamic Azad University of Iran, Tehran-South Branch, Iran

[*]Corresponding author E-mail: amonam111@gmail.com

https://doi.org/10.46649/fjiece.v3.2.17a.26.6.2024

Abstract. *The major challenge of data authenticity is how to check for image fraud, which creates a huge problem for the credibility of visual media. In this paper, we propose a method to investigate the performance of a Multilayer Perceptron (MLP) to extract the fraud images, this network is a class of supervised Artificial Neural Network (ANN. The proposal model applies MLP model to allocate extracted image features in order to distinguish them between real and modified contents. The examined features are included within statistical matrices, analysis of histogram space, and possible inequality that may arise during modifications. The proposed MLP was trained with dataset that contains both real and fraudulent images, thus allowing the model to extract knowledge from the original patterns that differentiate between those two classes. The model's performance was validated with several metrics, including accuracy, precision, and computational cost. Furthermore, this paper presents comparisons against traditional methods that were examined in the procedure. The finding of this work enhances the model with improved image fraud detection by showcasing the capabilities of MLPs within 162.59 seconds to 86% detection, while the base algorithm in 205.92 seconds succeeded in recognizing 82%.*

Keywords: *Image fraud; Deep Learning; MLP.*

1. INTRODUCTION

With the huge development of the digital age in this century, a new era of digital convenience has emerged, as the online transactions and document sharing have become more and more common [1], [2]. However, this convenience was accompanied by a concealed cost fact: an increased vulnerability to fraudulent activity. Recently, scammers have become very skilled at manipulating images, using advanced techniques to create fake documents. [3], change product images [4], and avoid traditional security protocols within system structure [5]. Traditional image fruad detection apply manual examination or algorithms that are based on exsisiting rules, which are unable to keep track with these strategies that are evolving constantly. The basic fundamental parameter which improves the status of these methods is the involving of Artificial Neural Netowrks (ANN). Actually, ANN models can obtain complex patterns from the trained dataset through their neurons. ANN models present exceptional proficiency in the identification of clear discrepancies in images [6], espacially in fraud detection field. To automatically identify data modifications, ANN models can be trained extensively with datasets which include both real and fraudulent images [7]. There are several advantages to transforming from manual feature annotitations to automated feature

learning [8]. With the presence of emergent fraud efforts, ANN models are able to gain the knowledge of such fraud with the absence of the need for human knowledge to identify specific manipulation techniques [9]. Furthermore, these models are able to manag a huge voluom of datasets, thus allowing them to accompulish high percentage of accuracy in image classification tasks, and overcoming traditional methods in this domain.

A diverse array of applications is made possible by the integration of deep learning and image processing. A robust and automated solution for combating image-based fraud, including the verification of the authenticity of identity documents and the protection of online financial transactions [10], is provided by deep learning. Fraud detection will be further improved by the continuous development of deep learning technology, thereby fostering a more secure and robust digital environment [11]. With the improvement of imaging equipment and image processing methods, a new branch of quality control and precision tools has emerged, and advanced image systems for measuring, calibrating, and controlling mechanical connections are introduced daily, improving image quality. Machine vision and image processing have become widely used in various fields [12], and their use in industrial product quality control, robot guidance, and automatic guidance is growing daily. Image processing involves receiving the image as a two-dimensional signal and using standard signal processing methods. Image processing is any signal processing that uses an image as input, such as a photo or movie scene.

Digital signatures and watermarks are embedded in images during creation. Images must be processed before these methods can be used. Passive methods can identify the same image without preprocessing it, unlike active methods. Photo fraud includes rotation, enlargement, noise addition, and noise removal from the body. Therefore, challenges such as data manipulation and signature forgante still remain as an open research problems.

Motivated by the above challenges, this paper presents a Multilayer Perceptron (MLP) [13] model to detect fraud in traditional images, in the training process, we included a 50 images divided as two groups with clean and fraud images. The detection process of MLP actually depends entirly on the changes in the pixel’s histogram, thus we include a cleaning process of the involved dataset as a first step in the preprocessing step.

2. RELATED WORK

The digital age has ushered in an era of unprecedented access to information and visual content. However, this scenario of ease of access also shows a huge challenge, including the rise of image fraud and data manipulation. Malicious users can now manipulate images and data with increasing sophistication, creating a crisis of trust issues in the information we consume.

One of the most common techniques for image fraud is photo editing software detection [14]. Subtle alteration of images can change a person's viewpoints, remove unwanted objects, or even create entirely new scenes. Deepfakes, a type of AI-generated video, pose a particularly dangerous threat. People can use deepfakes to create realistic videos of themselves saying or doing things they never did, potentially causing immense reputational damage or even swaying public opinion.

Data manipulation is also another type of digital deception. Here, one can fabricate or alter numbers and statistics to promote a specific agenda. This manipulation can lead to misleading conclusions and opinions. Furthermore, fraudulent data manipulation can also occur in financial markets, where it can be

used to inflate stock prices or mislead investors. The main consequences of image fraud and data manipulation are far-reaching; for instance, manipulated images can erode public trust in the media, political sphere, and other fields.

Artificial Intelligence has developed a Multilayer Perceptron (MLP) tool [13], which uses images as a primary input to perform tasks accurately. These image processors process images either as a single image or as a set of related variables, known as features. These features represent the characteristics of the image, and any changes in any image will modify these features, indicating that the image has been manipulated. Modern digital cameras and image editing software, such as Photoshop, make digital image creation easy. People often forge images to alter or conceal data without detection [14]. Copy-transfer forgery, a common type of image forgery, involves copying and pasting a portion of one photo into another. This has damaged the credibility of digital images in criminal investigations and applications. This type of fraud is harder to detect in image forgery because the copied part matches the background, color, and noise of other parts. Thus, images must be accurate before use as documentation. Traditional image forgery detection methods are active and passive, such as the SIFT-RANSAC method [15].

To that end, this work approaches the image fruad task as a learning-classification problem. By utilizing the learning parameters of the proposed MLP, the model is able to classify histogram pixels as either fruad or geinoin pixels, leading to a full extension to the target image.

3. METHOD

3.1. PROBLEM STATEMENT

Robust approaches for detecting fraudulent images are necessary due to the growing dependence on digital documents for tasks such as identity verification. Traditional algorithms have difficulty detecting complex forgeries, and manual examination is both laborious and prone to mistakes. When it comes to protecting online transactions and reducing the likelihood of fraud, nothing is more important than creating automated image processing algorithms that can reliably differentiate between real and altered photos. With the advent of information technology that facilitates the collection, storage and processing of huge amounts of data. Some of this data is images. Today, organizations need to detect fraud in image data to use it. Extracting meaning from the mass of data and using it for useful organizational purposes requires the use of advanced methods such as deep learning.

Deep learning is one of the function optimization methods that has been used in recent years to solve many complex and practical problems [16]. In problems where a simple analytical form for the objective function is not known, methods based on searching for optimal solutions in the space of possible solutions of the problem are especially used. Also, in cases where the number of optimization parameters for the given problem is large or includes a wide range of changes, and also in cases where multiple constraints and possibly unexpressable in the form of simple mathematical relationships can affect this problem.

3.2. ARTIFICIAL INTELLIGENT FOR IMAGE PROCESSING

In order to train their algorithms, deep learning takes cues from the way the human brain works. These models consist of multiple interconnected layers that process the input in a hierarchical fashion. Multilayer Perceptron's (MLP) capacity to directly extract features from visual data makes them ideal for

fraud detection within the framework of image processing [17]. Because of this capability, MLP can be employed to identify instances of fraud. Several techniques have been proposed for the identification and detection of fraudulent activities in images, with the utilization of deep learning emerging as a novel approach in detecting image forgery and fraud. Through conducting thorough investigations and extensive study, it was determined that this method exhibits superior performance compared to alternative ways. With the emergence of information technology that enables the gathering, retention, and manipulation of vast quantities of data. A portion of this material consists of images [18]. Currently, enterprises must be able to identify instances of fraudulent activity within picture data in order to utilize it effectively. To derive significance from a large amount of data and apply it effectively for organizational reasons, advanced techniques like deep learning are necessary.

Deep learning is a function optimization method that has been increasingly employed in recent years to address numerous intricate and real-world situations. When the objective function lacks a straightforward analytical form, techniques that include searching for optimal solutions inside the problem's solution space are commonly employed. In situations when the problem involves a large number of optimization parameters or encompasses a wide range of modifications, as well as scenarios where there are various restrictions that cannot be easily expressed using basic mathematical connections, this problem can be affected. Optimal image fraud detection planning is one of the most important aspect of fraud detection, which depends entirly on ANN models, with this unlimitted wide range of applications, fraud detection methods and algorithms methods which involve images and data can provide a serious threat. In order to commit financial crimes and / or modifying product photos on e-commerce platforms, the malicious users are constantly coming up with new approuches to access and fruad images and authentic data, such as altering identification documents, digital signiture modification, and date altering. Traditional image processing and computer vision techniques, which are based on hand-crafted features detection and extraction that are restricted with specific limitation and rules, have a difficult time keeping up with these constantly evolving strategies. One of the most effective methods for detecting fraudulent approaches based on images is MLP model [17], and in particular, it performe quite well. This model has the ability to learn automatically the most subtle parameters traits from datasets that identify real content from modified information, and present an output with user specified criteria.

In this study, we investigate the possibility of combining deep learning and image processing in order to detect fraudulent activity. Within this article, we go into the training process of a MLP model, explain the benefits of deep learning in comparison to more conventional methods, and investigate the potential applications of deep learning.

3.3. DATA PREPROCESSING

In the majority of real-world data mining applications, even with the vast amount of data and their storage locations, it is common to encounter missing values in the available samples. When dealing with huge data [19], it is important to not overlook missing samples, with the resolution entails substituting and purifying the data by utilizing predetermined values. This study applies the average data to substitute for the missing data. It signifies that the mean is calculated based on the existing data and any missing data is substituted.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Variances in the efficiency of feature modifications and the significant impact of higher values on other values do not necessarily indicate their importance. In order to resolve this issue, the dataset which used in the training process is subjected to normalization via linear normalization approach as follows:

$$X = 2 * \frac{x - min(x)}{mac(x) - min(x)} - 1 \qquad (1)$$

where $\min(x)$ and $\max(x)$ is the lower and the upper limits of the input vector x. The final outcome of Eq. 2 is the data that is normalized for learning task and obtain the features of the selected data. The approach of main components analysis can be considered as a means to reduce the dimensions of characteristics and their selection. One of the primary uses of principal component analysis is in classification for reducing dimensions and selecting features. The data principal component analysis method is used to map from the input space to the new data space. This strategy results in the loss of correlation between data dimensions and a significant increase in the dispersion across different classes. Through the utilization of principal component analysis, the research identified 8 specific features from the database in order to enhance the accuracy of sample classification.

3.4. IMPLEMENTATION

The Structure of MLP is presented in Fig. 1, where d_i and f_i are the input coefficients, w^1 is the weight of each input, $z_{n,m}^l$ is the number of the hidden layer, $A_{n.1}^L$ is the output layer, and $\hat{y}_n$ is the final output. The proposed MLP used for fraud image detection typically comprises the following layers:

- The input layer of a neural network receives the pre-processed image data, which is usually transformed into a one-dimensional vector.
- Four hidden layers consist of interconnected nodes that carry out non-linear transformations on the data. Tuning the hyperparameters of the number of hidden layers and the number of nodes within each layer is crucial.
- The output layer is responsible for representing the classification output. In binary classification, it usually consists of a single node that distinguishes between genuine and fraudulent cases. In multi-class classification, there are multiple nodes that classify different types of manipulations.
-

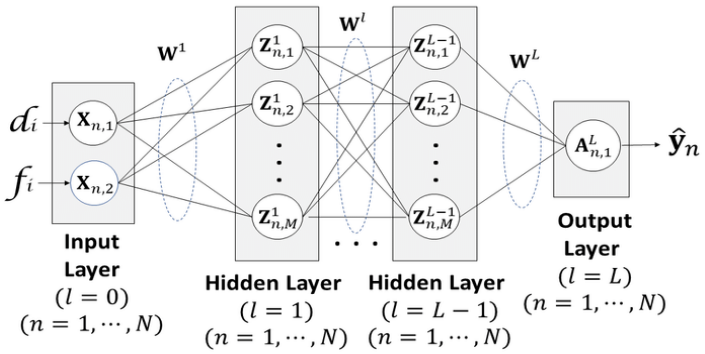

Fig. 1. Structure of the proposed MLP

3.5. TRAINING PROCESS

The MLP architecture is defined once the data is prepared. This design specifies the network's structure, down to the number and kind of layers. While there are a number of MLP architectures, most of them follow a standard pattern. In the middle, you'll find convolutional layers that are responsible for feature extraction from the images. The image is scanned by these layers, which apply learnable filters that identify patterns such as textures, forms, and edges. Various convolutional layers are used by the network to extract characteristics with varying degrees of granularity. Next, pooling layers are employed to lower the data's dimensionality, allowing the network to process it more efficiently in terms of computation. The classifier is performed lastly by fully linked layers. Using the information retrieved from the convolutional layers, they figure out if the image is real or not.

The training process starts once the data is prepared and the architecture is defined. The MLP receives the labeled dataset in batches. Every time around, the network makes a guess as to whether or not each picture in the batch is genuine. The error of the model is computed between the predicted value against the labeled actual data. This behavior is accomplished with the algorithm backpropagation become involved in the procedure. With this procedure, the basis weights are computed accordingly, where the predicted value keeps compared against the value from the neurons values every time, and the value of the prediction keeps in reduction till the model compute the finial minimized error between these two values. With this process, MLP can optimally the final value and make final decision on which image is real and which one is fraud.

When the model training is completed on the dataset, it quite important to assess the model performance with different subset of the dataset namely as test data, this test data is actually labeled the same as the training dataset, it should be noted that this dataset has not been imported to the model, with this approach, we will make sure that the assessment and validation is performed fairly. By this evaluation, the model exhibit the accuracy, precision, and recall on the new test dataset.

4. SIMULATION RESULTS AND DISCUSSION

4.1. SIMULATION SETTING

The proposed MLP model was simulated with MATAB software tool, the software was running on a personal Labtop with 3.2 GHz processor, 8 GB RAM memory, and 4 GB graphic processor memory. To minipulate the dataset, we utilize Photoshop CS8 software. The images utilized were sourced from graphic data repositories, specifically Shutterstock and National Geographic. The proposed method selected a collection of legitimate digital images in order to evaluate the effectiveness and dependability of it's performance in terms of the accuracy and identification of fraudulent activity in digital images. The statistical collection was used to choose and create fifty digital images, which were then manually selected. The modifications that were applied including copying, rotating, reducing the quality, changing to only a few pixels, compressing, and reducing the number of copied area. Subsequently, the proposed algorithm and the original algorithm were utilized to study the identification of fraud in two test images. Following

this, the reliability and efficiency of the approaches utilized on fifty test samples were evaluated in terms of their ability to detect fraud.

4.2. SIMULATION RESULTS

In order to test the efficiency and reliability of the proposed method in the accuracy and detection of fraud in digital images, a set of valid digital images was selected. From this statistical collection, 50 digital images were manually selected and forged. Changes made include copy, rotate, amount of copied area, reduce quality, change to just a few pixels and compress. In the following, the detection of fraud in two test images was investigated using the proposed algorithm and the original algorithm, and then the reliability efficiency of the methods used on 50 test samples was evaluated in detecting fraud. The purpose of SIFT-RANSAC algorithms is to identify distinctive features and sample photos. The implimintation of the proposed MLP was similiar to Chariot algorithm, where it used to obtain the matrix, and observed that the aforementioned method had a problem of being easily identified as a forgery. This was due to the differences in size between the version created to detect the forgery and the original image, as seen in the differential method. The SIFT-RANSAC algorithm is incapable of detecting fraud. However, in the proposed method, a distinct disparity was observed in a single node, which highlights the accuracy and efficiency of this approach. The proposed method demonstrated superior performance in the test samples where various fraudulent activities were conducted on the images. This research aims to employ the deep learning technique to provide a more robust evidence of the distinction between two images, a distinction that has already been established through the proposed method. Based on the non-uniformity observed in the graph resulting from the matrix analysis of the images, it was determined that the second image is distinct from the first image. This study aims to demonstrate the distinction between the authentic and altered image through meticulous analysis. The proposed method was utilized to perform this work, and the comparison of each method revealed that the accuracy of the proposed method is optimal. This was determined by analyzing the corresponding graph generated from each photo. The proposed method arranges and analyzes the graph associated with each of the photos. The disparity between the graphs pertaining to each image signifies the variation or deception in the images compared to one another. Furthermore, employing the suggested approach involved sampling each pixel of the image to compare and construct the corresponding graph. Ultimately, these constructed graphs exhibit the distinctive details and prominent characteristics of the images. After conducting a thorough analysis of the pixels and utilizing data mining techniques, it has been determined that the proposed method is both faster and more accurate. This is due to its ability to efficiently process the characteristic matrix of the images.

Fig. 2 presents the histogram of the original and manipulated images, which shows the changes in the pixel intensity level. On the right side of this figure, the histogram corresponding to the original image of the first input is seen, and on the left side, the histogram corresponding to the dummy image of the first input is seen. As shown in the diagram and as an example of the size of one of the pixels, here we have shown the pixel 500 for comparison, it can be seen that the intensity level of this pixel is different in the image on the left, which is related to the image. This level of pixels can confirm which image is manipulated and which one is genuine. In this manner, MLP can classify each image separately.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

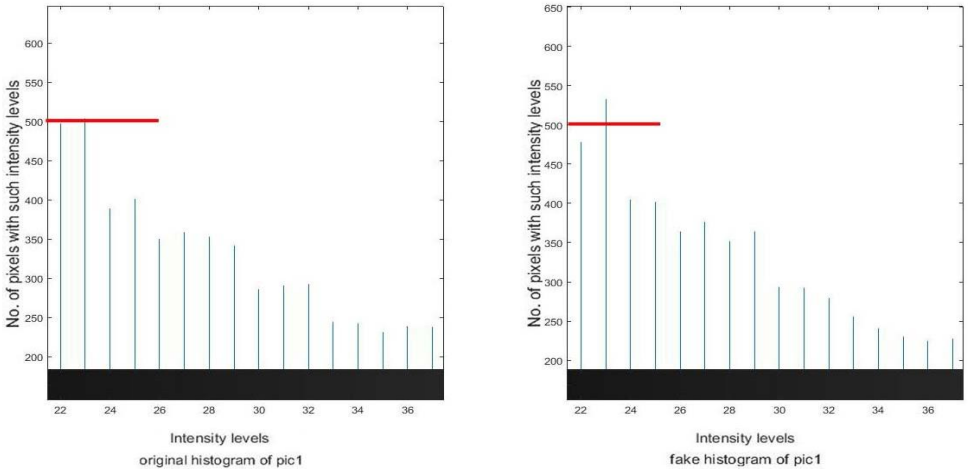

Fig. 2. Histogram of the original and fake image 1

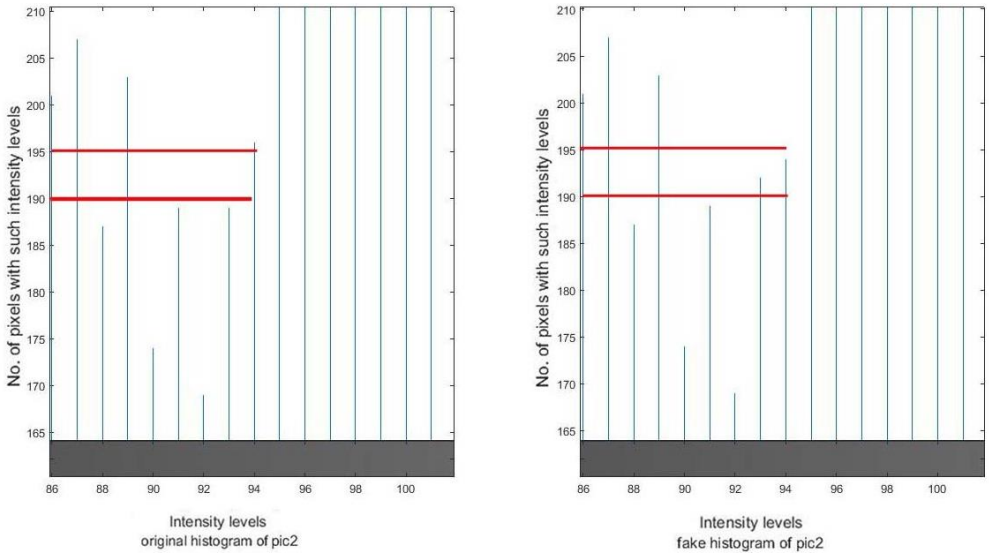

Fig. 3. Histogram of the original and fake image 2

In Fig. 3, the histogram related to the original image of the second input can be seen, and on the left side, the graph related to the histogram of the fake image of the second input can be seen. The same figure shown in the diagram, for example, the amount of two pixels, in this example, pixels 190 and 195 are compared, it can be seen that the brightness level of this pixel is different in the image on the left, which corresponds to the image on the right.

Table 1. Average productivity and accuracy percentage (for 50 images)

Method	Correct diagnose %	False diagnose %
Proposed method	86	14
Algorithm SIFT-RANSAC	82	18

To further depict the proposed method accuracy in detection fraud images, Table1 present a comparison on the performance of the proposed method against SIFT-RANSAC method [15], were it shown that the accuracy of the proposed method outperforms traditional method.

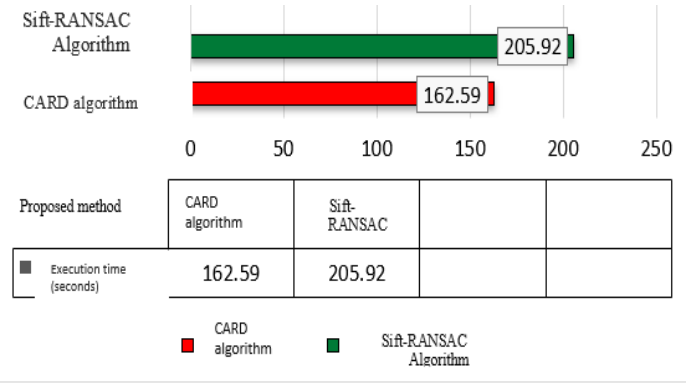

Fig. 4. Computational cost comparison

Furthermore, Fig. 4 present the computational cost of the proposed method, were it cost lower running time against SIFT-RANSAC method. On the other hand, the performance of the proposed MLP, which are a fundamental form of Artificial Neural Network, possess significant learning capabilities but can be computationally demanding to train. Although MLPs are efficient in solving complex problems, the large number of weights and activation functions in the network results in computationally intensive calculations during the backpropagation process, which is the training algorithm. The computational expense of MLPs can restrict their use to large datasets or real-time applications. Continued research is being conducted to tackle this challenge, which involves investigating effective hardware implementations, refining training algorithms, and employing methods such as weight pruning to decrease network complexity. The addressing of the model computational constraints, it can retain the efficacy as a machine learning tool while also becoming more scalable and applicable to real-world situations.

5. CONCLUSIONS

This peper presents a MLP model to detect fraud in digital images. This was determined by analyzing the corresponding graph generated from each image. The proposed method arranges and analyzes the graph associated with each of the photos. The disparity between the graphs associated with each image signifies the divergence or deception in the images compared to one another. Additionally, the suggested approach involved sampling each pixel of the image to compare and construct the corresponding graph. Ultimately, these graphs reveal the distinct details and prominent characteristics of the images. After conducting a thorough analysis of the pixels and utilizing data mining techniques, it has been determined that the proposed method is both faster and more accurate. This is due to its ability to efficiently process the characteristic matrix of the images.

6. REFERENCES

[1] F. Z. Mehrjardi, A. M. Latif, M. S. Zarchi, and R. Sheikhpour, “A survey on deep learning-based image forgery detection,” *Pattern Recognit*, p. 109778, 2023.

[2] C. Atal, M. Angala, F. R. Fernandez, and C. K. Lacsina, "Electronic Document Flow Monitoring And Control System Using Document Structure Analysis," *ECS Trans*, vol. 107, no. 1, p. 20169, 2022.

[3] L. Korsell, "Fraud in the Twenty-first Century," *Eur J Crim Pol Res*, vol. 26, no. 3, pp. 285–291, 2020.

[4] B. Garrett *et al.*, "Internet health scams—Developing a taxonomy and risk-of-deception assessment tool," *Health Soc Care Community*, vol. 27, no. 1, pp. 226–240, 2019.

[5] A. Dell'Aquila, "Digital imaging information technology applied to seed germination testing. A review," *Agron Sustain Dev*, vol. 29, pp. 213–221, 2009.

[6] H. Yu, L. T. Yang, Q. Zhang, D. Armstrong, and M. J. Deen, "Convolutional neural networks for medical image analysis: state-of-the-art, comparisons, improvement and perspectives," *Neurocomputing*, vol. 444, pp. 92–110, 2021.

[7] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of digital forensic research workshop*, Cleveland, OH, 2003, pp. 652–663.

[8] G. Zhu, Y. Zheng, D. Doermann, and S. Jaeger, "Signature detection and matching for document image retrieval," *IEEE Trans Pattern Anal Mach Intell*, vol. 31, no. 11, pp. 2015–2031, 2008.

[9] M. Hamilton *et al.*, "Flexible and scalable deep learning with MMLSpark," in *International Conference on Predictive Applications and APIs*, PMLR, 2018, pp. 11–22.

[10] J. M. Blackledge and E. Coyle, "e-Fraud Prevention based on the Self-Authentication of e-Documents," in *2010 Fourth International Conference on Digital Society*, IEEE, 2010, pp. 329–338.

[11] V. Shah, "Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats," *Revista Espanola de Documentacion Cientifica*, vol. 15, no. 4, pp. 42–66, 2021.

[12] A. Martin and S. Tosunoglu, "Image processing techniques for machine vision," *Miami, Florida*, pp. 1–9, 2000.

[13] M.-C. Popescu, V. E. Balas, L. Perescu-Popescu, and N. Mastorakis, "Multilayer perceptron and neural networks," *WSEAS Transactions on Circuits and Systems*, vol. 8, no. 7, pp. 579–588, 2009.

[14] R.-Y. Sun, "Optimization for deep learning: An overview," *Journal of the Operations Research Society of China*, vol. 8, no. 2, pp. 249–294, 2020.

[15] G. Shi, X. Xu, and Y. Dai, "SIFT feature point matching based on improved RANSAC algorithm," in *2013 5th International Conference on Intelligent Human-Machine Systems and Cybernetics*, IEEE, 2013, pp. 474–477.

[16] L. Bian, L. Zhang, K. Zhao, H. Wang, and S. Gong, "Image-based scam detection method using an attention capsule network," *IEEE Access*, vol. 9, pp. 33654–33665, 2021.

[17] M.-C. Popescu, V. E. Balas, L. Perescu-Popescu, and N. Mastorakis, "Multilayer perceptron and neural networks," *WSEAS Transactions on Circuits and Systems*, vol. 8, no. 7, pp. 579–588, 2009.

[18] J. Hurník, A. Zatočilová, D. Koutný, and D. Paloušek, "Enhancing the accuracy of forging measurement using silhouettes in images," *Measurement*, vol. 194, p. 111059, 2022.

[19] N. Sidere, F. Cruz, M. Coustaty, and J.-M. Ogier, "A dataset for forgery detection and spotting in document images," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, IEEE, 2017, pp. 26–31.