Detecting Fake Images on Social Media using Machine Learning

Njood Mohammed AlShariah¹, Abdul Khader Jilani Saudagar²
Information Systems Department, College of Computer and Information Sciences
Imam Mohammad Ibn Saud Islamic University (IMSIU)
Riyadh, Saudi Arabia

Abstract—In this technological era, social media has a major role in people’s daily life. Most people share text, images, and videos on social media frequently (e.g., Twitter, Snapchat, Facebook, and Instagram). Images are one of the most common types of media share among users on social media. So, there is a need for monitoring and detecting images and manipulate them. This research aimed to propose an approach to extracting image content, classify it, and verify the authenticity of digital images and uncover manipulation. Instagram is one of the most important websites and mobile image sharing applications on social media. This allows users to take photos, add digital photographic filters and upload pictures. There are many unwanted contents in Instagram’s posts such as threats and forged images, which may cause problems to society and national security. This research aims to build a model that can be used to classify Instagram content (images) to detect any threats and forged images. The model is built using deep learning algorithms, which is Convolutional Neural Network (CNN). Alexnet network and transfer learning using Alexnet. The results showed that the model could classify Instagram content (images) to detect any threats and forged images. The results of this research will be helpful in monitoring and tracking the shared images in social media for unusual content and forged images detection and to protect social media from electronic attacks and threats.

Keywords—Convolution Neural Network (CNN); Image forgery; Classification; Alexnet; Rectified Linear Unit (ReLU); SoftMax function; Features extraction

I. INTRODUCTION

It is a fact that social media have changed the way people interact and carry on with their everyday lives. Social networking sites are a prominent media phenomenon nowadays, and have attracted a large number of people. Worldwide, the number of users [1] now exceeds three billion. In the Gulf region, growth in the number of active users has exceeded 66% [2]. Saudi Arabia ranks seventh in the world in terms of social media use; more than 75% of its estimated 25 million people [3] are active users of social media. Social media are based on specific foundations that bring people together and empower them to express themselves, share their interests and ideas, and forge new friendships with others who share their interests. Facebook, Twitter, and Instagram are among the most popular social networking sites of the day. It is a widespread practice to share images online through social networking services such as Instagram. At least 80 million images [4] are currently shared via Instagram every day. Instagram enables users to take photographs, apply digital photographic filters, and upload the pictures to website for social networking together with short captions. People upload and share billions of pictures [5] every day on social media.

A huge number of people have become victims of photo forgery in this technological age. Some criminals use software to exploit and use pictures as evidence to confuse the courts of justice [17]. To put an end to this, all photographs exchanged via social media should be labeled as true or fake. Social media is a great platform for knowledge sharing and dissemination. Yet If there is no caution, people may be fooled and even induced by unintended false propaganda. Though most image editing using Photoshop is clearly evident, some of these images may indeed appear really due to pixelization and shoddy jobs by novices [16]. In particular, in the Policy arena, edited images can break the credibility of a politician. In this research using machine learning algorithms [6, 7], the researcher will attempt to propose a classifier model via a convolutional neural network (CNN) that is capable of take advantage of knowledge to take an image from social media and then classify and detect it.

This research proposes an approach that takes an image as input and classifies it, using an effective system (the CNN model) [20]. The result of this proposed research will be helpful in monitoring and tracking social media content and in discovering fraud on social networking sites, especially in the field of images.

II. LITERATURE REVIEW

Very little work has been finalized around detecting forge audio, images, and videos. Yet, several studies and tasks are underway to identify what can be done around the incredible proliferation about counterfeit pictures online. Adobe recognizes the way in which Photoshop is misused and has tried to offer a sort of antidote [8]. The following provide a summary of a few of these studies:

According to a study [9] conducted by Zheng et al. (2018), the identification of fake news and images is very difficult, as fact-finding of news on a pure basis remains an open problem and few existing models can be used to resolve the problem. It has been proposed to study the problem of “detecting fake news." Through a thorough investigation of counterfeit news,
many useful properties are determined from text words and pictures used in counterfeit news. There are some hidden characteristics in words and images used in fake news, which can be identified through a collection of hidden properties derived from this model through various layers. A pattern called TI-CNN has been proposed. By displaying clear and embedded features in a unified space, TI-CNN is trained with both text and image information at the same time.

Raturi’s 2018 architecture [10] was proposed to identify counterfeit accounts in social networks, especially on Facebook. In this research, a machine learning feature was used to better predict fake accounts, based on their posts and the placement on their social networking walls. Support Vector Machine (SVM) and Complement Naïve Bayes (CNB) were used in this process, to validate content based on text classification and data analysis. The analysis of the data focused on the collection of offensive words, and the number of times they were repeated. For Facebook, SVM shows a 97% resolution where CNB shows 95% accuracy in recognizing Bag of Words (BOW)-based counterfeit accounts. The results of the study confirmed that the main problem related to the safety of social networks is that data is not properly validated before publishing.

In 2017 study by Bunk et al [11], two systems were proposed to detect and localize fake images using a mix of resampling properties and deep learning. In the initial system, the Radon conversion of resampling properties is determined on overlapping pictures corrections. Deep learning classifiers and a Gaussian conditional domain pattern are then used to construct a heat map. A Random Walker segmentation method uses total areas. In the next system, for identification and localization, software resampling properties are passed on overlapping object patches over a long-term memory (LSTM)-based network. In addition, the detection/ localization performance of both systems was compared. The results confirmed that both systems are active in detecting and settling digital image fraud.

Aphiwongsophon and Chongstitvatana [12], aimed to use automated learning techniques to detect counterfeit news. Three common techniques were used in the experiments: Naïve Bayes, Neural Network and Support Vector Machine (SVM). The normalization method is a major step to disinfect data before using the automatic learning method to sort information. The results show Naïve Bayes to have a 96.08% accuracy in detecting counterfeit news. There are two other advanced methods, the Neural Network Machine and the Support Network (SVM), which achieve 99.90% accuracy.

In [13] by Kuruvilla et al., a neural network was successfully trained by analyzing the 4000 fake and 4000 real images error level. The trained neural network has succeeded in identifying the image as fake or real, with a high success rate of 83%. The results showed that using this application on mobile platforms significantly reduces the spread of fake images across social networks. In addition, this can be used as a false image verification method in digital authentication, court evidence assessment, etc. It develops and tests reliable fake image detection program by combining the results of metadata analysis (40%) and neural network output (60%).

According to [15] Kim’s and Lee’s, digital forensics techniques are needed to detect manipulation and fake images used for illegal purposes. Thus, the researchers in this study have been working on an algorithm to detect fake images through deep learning technology, which has achieved remarkable results in modern research. First, a converted neural network is applied to image processing. In addition, a high pass filter is used to get at hidden features in the image instead of semantic information in the image. For experiments, modified images are created using intermediate filter, Gaussian blurring, and added white Gaussian noise.

This research develops an approach that takes an image as input and classifies it, using the CNN model. For a completely new task/problem, CNNs are very good feature extractors. It extracts useful attributes from an already trained CNN with its trained weights by feeding your data at each level and tuning the CNN a bit for the specific task. This means that a CNN can be retrained for new recognition tasks, enabling to build on pre-existing networks. This is called pre-training, where one can avoid training a CNN from the beginning and save time. CNN can carry out automatic feature extraction in the given task. It eliminates the need for manual feature extraction, since the features are learned directly by the CNN. In terms of performance, CNNs outperform many methods for image recognition tasks and many other tasks where it gives a high accuracy and accurate result. Another key feature of CNNs is weight sharing, which basically means that the same weight is used for two layers in the model. Due to the above features and advantages, CNN is used in this research in comparison to other deep learning algorithms.

III. RESEARCH METHODOLOGY

This research explores a supervised machine learning classification problem [14,18], where the label or category of the input sample is known as the training phase. There are two labels or classes: the original image class and the fake image class. The researcher uses the deep learning technique via a conventional neural network (CNN).

A. Input Features for Neural Networks

Features in a neural network are the variables or attributes in the data set where extraction of features is a fundamental step in automated methods based on approaches to machine learning. The goal is to obtain useful data characteristics. In order to classify images, convolution neural networks use features. Such features are taught by the network during the training process itself. Features aim to reduce the number of features in a dataset by creating new features from the existing ones (and then discarding the original features). Then this new simplified set of features should be able to summarize most of the details in the original set of features. Therefore, from a combination of the original set, a condensed version of the original features can be produced.

B. Developing Fake Image Detection Algorithm Architecture

Convolution neural network (CNN) architecture is illustrated in Fig. 1.

- Target images will be extracted from the Instagram application, where these images represent the dataset
that is relevant to find answers to the research questions, test the hypothesis and assess the results.

- Construct CNN convolution layer, the convolutional layer is responsible for extracting image features, using conventional mathematical operations. These convolutional operations act as applying digital filters with two dimensions. Assuming the image tile is 4X4 pixels and the conventional filter is 2X2 matrix filter, the Fig. 2, Fig. 3 and Fig. 4 illustrates the conventional operation, where each image tile block matrix with dimensions equal to the filter dimension will be multiplied by the filter matrix.

- Construct the Activation function. Fig. 5 illustrates the activation function layer, contained in the yellow oval. The activation function layer is a layer between the conventional layer and the feature map, which, as in any traditional neural network activation function, removes un-wanted pixels, e.g. negative values.

- Due to the nonlinear nature of image data, the researcher will use a non-linear activation function called The Rectified Linear Unit (ReLU). The rectifier job is defined as the positive section of its argument, as shown in the Fig. 6.

- To reduce the size of the array in the precise step, we downsample it using an algorithm called max pooling to modify the output of the layer. Further pooling helps to make the representation almost invariant with respect to small translations of the input.

Fig. 7 illustrates the max pooling operation on an image tile example with max pooling at a 2X2 dimension size:

- Make a prediction, this neural network decides whether the image is, or is not, a match. To differentiate it from the convolution process, it is referred to as a “fully connected” network. Before constructing a fully connected network, the pooled feature map data must convert to the single column to be suitable as a neural network input. This process is known as “flattening,” as shown in the Fig. 8.

- Fig. 9 illustrates the fully connected network architecture.
training data are extracted from the original images and, for each original image, three fake images were made. The researcher modified the original images via addition, deletion, changing colors. The dataset training steps are described as follow by using CNN network.

1) Load and analyze image data: Load the data of the sample as a data store for the image. Image Datastore automatically labels images based on the name of the folder and stores the data as an object of the image datastore. An image datastore helps you to store large image information when training a convolution neural network and interpret image batches efficiently.

2) Define the network architecture: Determine the convolutional neural network architecture and create network layers.

3) Define training options: Defines the training options after defining the architecture of the network. Learning rate, number of epochs, momentum and batch size.

4) Train the network: Train the network using layer-defined architecture, training data & the training options.

5) Predict the labels of new data and measure the classification accuracy.

Predict the labels of the data using the trained network, and measure the final accuracy.

Note that Alexnet network and Transfer Learning network follow the same training steps but with some additions where the load pretrained network is additional step in Alexnet network and the replace final layers is additional step in transfer learning.

B. Test Datasets

In this step the researcher used codes to choose an image from amongst the images; then it determines whether the image is original or fake as shown in Fig. 10 and Fig. 11.

IV. IMPLEMENTATION

Applying MATLAB software with the Deep Learning Toolbox helps you to train your own CNN from scratch or use a pretrained model to conduct transfer learning. The method you choose depends on the resource you have, the type of application you are creating and the purpose of the application. In order to train the network from scratch, the number of layers and filters must be determined and the other requirements adjusted. Training a specific model from the start also requires enormous amounts of data, based on millions of samples, which can take a long time. An appropriate alternative to CNN training from scratch is the use of a pre-training model to automatically extract properties from a new dataset. Known as transfer learning, this is an easy way to apply deep learning without a great data set and a long period spent on calculation and training.

A. Create Simple Deep Learning Networks for Classification

There are three networks: Alexnet, Classic CNN, and Alexnet using transfer learning. For each network, there are a training dataset and a test dataset. There are also cases in which the test data is from training data and vice versa. There are two datasets in our experiment. The first dataset contains 1400 images for training and 400 images for testing. The second dataset contains 400 images for training and 40 images for testing. In the second dataset, the fake images in the
V. RESULTS AND DISCUSSION

The performance measures of the proposed methodology are discussed in detail. The major goal of this work is to detect both normal and fake images in an accurate manner. For this purpose, a convolution neural network is utilized in this work. This CNN comprises four layers: the convolution layer, pooling layer, activation layer, and SoftMax layer. Each layer performs a specific task individually. First, the input image is obtained from the image acquisition. Then the image is converted into non-overlapping patches, from these patches. Further, the values of the features are normalized and down sampled to obtain a reduced feature set. Finally, the probability of the output is determined to classify the given image as normal or fake. Here, the approach developed in this research is evaluated, based on performance metrics and relative with the current techniques.

A. Performance Measures

The performance of the anticipated methodology is evaluated using different performance metrics, such as sensitivity, specificity, accuracy, precision, and recall.

1) Sensitivity

Sensitivity refers to the calculation of the ratio of True Positives that are recognized accurately. It can be defined as,

\[ \text{Sensitivity} = \frac{TP}{TP+FN} \]  

2) Specificity

Specificity is defined as the ratio of correctly detected True Negatives. This can be defined as,

\[ \text{Specificity} = \frac{TN}{TN+FP} \]  

3) Accuracy

Accuracy is known as the ratio of correct intrusions of classification to the total number of data. It is clarified as follows,

\[ \text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \]  

4) Precision

Precision is the ratio of the number of intrusions that are correctly identified to the total number of intrusions in the process. This is denoted by,

\[ \text{Precision} = \frac{TP}{TP+FP} \]  

5) Recall

Recall is the ratio of the number of properly detected intrusions to the number of intrusions that are relevant. This can be represented as,

\[ \text{Recall} = \frac{TP}{TP+FN} \]  

B. Performance Analysis

The quality of the technique proposed is tabulated and shown in the tables below. The accuracy of the results is shown to vary among networks. Alexnet is the most accurate, followed by Alexnet using TL and then Classic CNN. Table I illustrates comparison among three network types (Alexnet Network, Alexnet Using Transfer Learning, and Classic CNN) regarding the performance accuracy of results when testing data is from outside the training data. The findings reveal differences among the three networks, in favor of Alexnet (93.4), followed by Alexnet using transfer learning (93.2) and, finally, classic CNN (70.1). The findings also reveal differences among the three networks when testing data from the training data. These are again in favor of Alexnet (99.3), followed by Alexnet using transfer learning (94.0) and, finally, classic CNN (83.9). The results in the table below are specific to the first dataset.

Fig. 12 illustrates Mean scores of performance accuracy results, when testing data from outside the training data and from the training data.

Table II compares among the three network types (Alexnet Network, Alexnet Using Transfer Learning, and Classic CNN) regarding the performance accuracy of results when testing data from outside the training data. The findings reveal no statistically significant differences in the performance accuracy of results among the three network types. The value of significance level amounted to 0.172; this means it is greater than 0.05, which is not statistically significant. There were, however, differences amongst the three networks when testing data from the training data, in favor of Alexnet (91.1), followed by Alexnet Using Transfer Learning (78.4) and, finally, Classic CNN (64.5). The results in the table below are specific to the second dataset.

### TABLE I. KRUSKAL-WALLIS TEST OF THE DIFFERENCES BETWEEN THE MEAN SCORES OF PERFORMANCE ACCURACY RESULTS WHEN THE TESTING DATA IS FROM OUTSIDE THE TRAINING DATA AND FROM THE TRAINING DATA (ALEXNET, TL, CLASSIC CNN)

| Performance results when testing data is | Mean | SD | Chi-Square | P value |
|----------------------------------------|------|----|------------|---------|
| Outside the training data               |      |    |            |         |
| Alexnet Network                         | 93.4 | 2.0| 9.482      | 0.009   |
| Alexnet Using Transfer Learning         | 93.2 | 3.08|           |         |
| Classic CNN                             | 70.1 | 0.22|           |         |
| From the training data                  |      |    |            |         |
| Alexnet Network                         | 99.3 | 0.45| 12.635     | 0.002   |
| Alexnet Using Transfer Learning         | 94.0 | 0.93|           |         |
| Classic CNN                             | 83.9 | 3.17|           |         |

Fig. 12. Mean Scores of Performance Accuracy Results, when Testing Data from Outside the Training Data and from the Training Data.
TABLE II. KRUSKAL-WALLIS TEST OF THE DIFFERENCES BETWEEN THE MEAN SCORES OF PERFORMANCE ACCURACY RESULTS WHEN TESTING DATA FROM OUTSIDE THE TRAINING DATA AND FROM THE TRAINING DATA (ALEXNET, TL, CLASSIC CNN)

| Performance results when testing data from | Mean | SD  | Chi-Square | p. value |
|------------------------------------------|------|-----|------------|----------|
| Outside the training data                |      |     |            |          |
| Alexnet Network                           | 80.9 | 9.5 |            |          |
| Alexnet Using Transfer Learning          | 66.2 | 21.7| 3.519      | 0.172    |
| Classic CNN                              | 64.8 | 16.8|            |          |
| From the training data                   |      |     |            |          |
| Alexnet Network                           | 91.1 | 3.4 |            |          |
| Alexnet Using Transfer Learning          | 78.4 | 17.6| 7.559      | 0.023    |
| Classic CNN                              | 64.5 | 25.8|            |          |

Fig. 13 illustrates Mean scores of performances accuracy results when testing data from outside the training data and from the training data.

After running the code, the values of precision, recall, accuracy, specificity, and sensitivity are extracted from the confusion matrix by calculating the value of True positive, True Negative, False positive and False Negative for example in Alexnet network the confusion matrix shown in Table III.

From the above table the values are calculated where accuracy is 93.3, precision is 95.5, recall is 91.4, specificity is 95.3 and sensitivity is 91.4.

The performance of Alexnet, CNN, and TL is evaluated using several measures, such as accuracy, sensitivity, specificity, precision, recall, true positive rate, and true negative rate [19]. The performance of the methodologies is also evaluated and compared with current techniques. From the outcomes, it is concluded that the proposed Alexnet approach offers more accurate detection of fake images compared to conventional techniques. This proves the superiority of the developed methodology.

TABLE III. CONFUSION MATRIX OF ALEXNET NETWORK

| n = 400 | Actual Fake | Actual Normal |
|---------|-------------|---------------|
| Predicted Fake | TN 182 | FP 9 |
| Predicted Normal | FN 18 | TP 191 |

VI. CONCLUSION

Recently, electronic attacks have spread in Saudi Arabia. There is currently no clear vision nor a unified framework to protect us against the dangers of piracy and threats, especially about the penetration of social media and the spread of false accounts. This has led Saudi Arabia to invest in information security, which is concerned with protecting the technical infrastructure from hacking and focuses on developing techniques and tools to protect social media from electronic attacks and threats. This research has contributed to the rapid detection of fraud in social media, especially in the field of images, thus solving the problem of spreading rumors and promoting false news on social networking sites and helps communities seeking to protect their technical infrastructure from piracy and cyber threats and to strengthen their information security, where the crime of image forgery poses a danger to societies. There are some problem and limitations in neural networks including it computationally expensive, requiring the use of powerful and distinct processing units. Without a good CPU, neural networks are quite slow to train for complex tasks.

Another problem with neural networks is that they depend on the amount of data provided to them. If the quantity of data is small, then one can expect poor network performance and vice versa. Neural networks contain millions of parameters that require a huge amount of data. The use of neural networks thus requires a large amount of training data and takes time to train these neural networks.

It is clear—from the results of the model used—that a large, deep convolutional neural network is capable of achieving record-breaking results on a highly challenging dataset using supervised learning where the results of this research achieved high accuracy of up to 97%. The results of this research will be helpful in monitoring and tracking social media content and in discovering fraud on social networking sites, especially in the field of images. To effectively identify objects, the convolution neural network architecture implicitly combines the benefits obtained from standard neural network learning with the convolution process. Like a neural network, CNN and its variants can also be optimized to large datasets, which is often the case when classifying objects.

The recommendations for future work are for example using a more complex and deeper model for unpredictable problems. Integration of deep neural networks with the theory of enhanced learning, where the model is more effective. Neural network solutions rarely take into account non-linear feature interactions and non-monotonous short-term sequential patterns, which are necessary to model user behavior in sparse sequence data. A model may be integrated with neural networks to solve this problem. The dataset could be increased and another type of images could be used for training, for example gray-scale images.
REFERENCES

[1] G. Mohamed Sikandar, "100 Social Media Statistics You must know," [online] Available at: https://blog.statusbrew.com/social-media-statistics-2018-for-business/ [Accessed 02 Mar 2019].

[2] Damian Radcliffe, Amanda Lam, "Social Media in the Middle East," [online] Available at:https://www.researchgate.net/publication/323185146_Social_Media_in_the_Middle_East_The_Story_of_2017 [Accessed 06 Feb 2019].

[3] GMI_BLOGGER, "Saudi Arabia Social Media Statistics," GMI_blogger, [online] Available at:https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/ [Accessed 04 May 2019].

[4] Kit Smith, "49 Incredible Instagram Statistics," Brandwatch, [online] Available at: https://www.brandwatch.com/blog/instagram-stats/ [Accessed 10 May 2019].

[5] Selling Stock. (2014). Selling Stock. [online] Available at: https://www.selling-stock.com/Article/18-billion-images-uploaded-to-the-web-everyday [Accessed 12 Feb 2019].

[6] Li, W., Prasad, S., Fowler, J. E., & Bruce, L. M. (2012). Locality-preserving dimensionality reduction and classification for hyperspectral image analysis. IEEE Transactions on Geoscience and Remote Sensing, 50(4), 1185–1198.

[7] A. Krizhevsky, I. Sutskever, & G. E. Hinton, (2012). Imagenet classification with deep convolutional neural networks. In Advances in Neural Information Processing Systems, 1097–1105.

[8] K. Ravi, (2018). Detecting fake images with Machine Learning. Hakuch Journal

[9] L. Zheng, Y. Yang, J. Zhang, Q. Cui, X. Zhang, Z. Li, et al. (2018). TI-CNN: Convolutional Neural Networks for Fake News Detection. United States

[10] R. Raturi, (2018). Machine Learning Implementation for Identifying Fake Accounts in Social Network. International Journal of Pure and Applied Mathematics, 118(20), 4785–4797.

[11] J. Bunk, J. Bappy, H. Mohammed, T. M. Nataraj, L. Flenner, A., Manjunath, B., et al. (2017). Detection and Localization of Image Forgeries using Resampling Features and Deep Learning. University of California, Department of Electrical and Computer Engineering, USA.

[12] S. Apisitwongsuphon, & P. Chongstitvatana, (2017). Detecting Fake News with Machine Learning Method. Chulalongkorn University, Department of Computer Engineering, Bangkok, Thailand.

[13] M. Villan, A. Kuruvilla, K. J. Paul, & E. P. Elias, (2017). Fake Image Detection Using Machine Learning. IRACST—International Journal of Computer Science and Information Technology & Security (IJCSITS).

[14] S. Shalev-Shwartz, & S. Ben-David, (2014). Understanding Machine Learning: From Theory to Algorithms. New York: Cambridge University Press.

[15] D.-H. Kim, & H.-Y. Lee, (2017). Image Manipulation Detection using Convolutional Neural Network. International Journal of Applied Engineering Research, 12(21), 11640-11646.

[16] M. D. Ansari, S. P. Ghera, & V. Tyagi, (2014). Pixel-based image forgery detection: A Review. IETE Journal of Education, 55(1), 40–46.

[17] D. Strigl, K. Kofler, & S. Podlipnig, (2010). Performance and scalability of GPU-based convolutional neural networks. In 18th Euromicro Conference on Parallel, Distributed, and Network-Based Processing.

[18] Y. Li, & S. Cha, (2019). Face Recognition System. arXiv preprint arXiv:1901.02452.

[19] R. Kohavi, (1995, August). A Study of cross-validation and bootstrap for accuracy estimation and model selection. In Ijcai, 14(2), 1137–1145.

[20] R. Saracco, (2018). Detecting fake images using artificial intelligence. IEEE Future Directions.

www.ijacsa.thesai.org