International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Signify: Signature Verification Technique using Convolutional Neural Network

Alexandra Mae C. Laylo, Mark Daryl A. Decillo, Louie Andrew F. Boo, Jeffrey S. Sarmiento

Abstract: ***Signature is one of the biometric traits that are being used in person authentication and due to its dominant usage; it became one of the top subjects of forgery. In this study, a signature verification using Convolutional Neural Network (CNN) is proposed. With the use of transfer learning, inception-v3 is mainly used for the feature extraction of data samples and for classification of signatures. The proposed method is assessed on dataset of handwritten signatures gathered from 4 people with 100 signatures each. The testing results determine the threshold value which is 96.43%. Factors that affect the accuracy of the result were also identified.***

Index Terms**: *Convolutional Neural Network, Inception, Signature Verification, Transfer Learning***

I. INTRODUCTION

Personal authentication methods are widely used nowadays and being implemented to better identify a certain individual. PINs and biometrics were commonly used but, still, human signature is the one being widely-used and accepted as a way of authentication [1].

Handwritten signature is a behavioral biometric trait that is acquired by a person over a period of time and becomes their unique identity. It is one of the significant biometric authentications under the behavioral characteristics [2]. It is not only considered as an individual trait, but also widely used in almost in legal activities, especially in documents, which serve as the proof of ownership of a person involved in such documents. These documents include banking, academic purposes, those that are property related, as well as those for duties and responsibilities. In creating a bank account, one will be asked for signature. In contracts there will always be a space provided for a signature.

Due to dominant usage, signatures gained high legal acceptance in the society. In that case, it became one of the top subjects of forgery.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Alexandra Mae C. Laylo*, BS Computer Engineering graduate, Batangas State University, Batangas City, Philippines.
Mark Daryl A. Decillo, BS Computer Engineering graduate, Batangas State University, Batangas City, Philippines.
Louie Andrew F. Boo, BS Computer Engineering graduate, Batangas State University, Batangas City, Philippines.
Jeffrey S. Sarmiento, Computer Engineering Department, College of Engineering, Architecture and Fine Arts, Batangas StateUniveristy, Batangas City, Philippines.

Forgery is the act of falsification or illegal reproduction of documents and contracts including signature of a person. There are three types of signature forgery. First is the random forgery, this type of forgery is the easiest to identify since the forger creates their own version of a signature based on the owner's name. Second type of forgery is the simple forgery wherein the forger imitates the signature with the knowledge of the original signature though without enough practice. And last is the skilled forgery, which is almost the same with the genuine signature [3], [4], and [5].

The range of issues of signature forgery, signature verification has come into action. It is a technique developed to differentiate forged signatures from genuine signatures. For the past years, the process of verification is being done manually through template matching which takes at least 2 to 20 minutes for every transaction – a very time-consuming process. Later on, automated signature verification was developed and has been used in some banking systems. There are two methods in data acquisition, the *offline mode* and *on-line mode.* In general signatures to be verified using offline mode are digitalized through the use of digital scanner or camera [4] and [5], whereas in on-line mode signatures are acquired with the use of digitalizing tablet [4].

Aside from signature forgery, another problem regarding to signature verification is the inconsistencies between signatures of an individual. Physiological state of a person, age, mood, body position and environment are just some factors that causes for a person to have variation in their signatures [6]. Due to this, even a genuine signature was being classified as forged signature.

Reference [4] focuses on the discussion of a certain technique in signature verification digitally done through the use of Artificial Neural Networks, specifically the feedforward neural network which was one of all its types. The method presented in the study was the optimization of the existing types of neural network. With the pattern recognition, it offered the usage of the so-call data structure tree as well as the nodes which were human-eye like. It also undergone several ways such as pre-processing, image scaling, normalization and other common ways of image processing for better recognition, for its implementation

The study was related in the researchers' study for both used neural network for the idea of signature verification. The only difference is, [4] used the feedforward type of neural network and the other used the convolutional neural network which is good to compare the results obtained upon the usage of both. In this study, the researchers specifically aimed to develop a signature verification technique using Convolutional Neural Network (CNN),

create software that incorporates convolutional neural network for signature verification, and identify factors that affect the accuracy of the tested signatures in signature verification process.

II. METHODOLOGY

A. Convolutional Neural Network

Convolutional neural network is one of the main classes of artificial neural network which are widely used in artificial image processing. According to [7], it is an effective way in image recognition and processing. It was described as an effective way in identifying faces, traffic signs as well as objects apart from vision empowering in automated driving cars and also robots.

The main purpose of convolution when it comes to the study of convolutional neural networks is for the feature extraction from the acquired image. It has the main feature of preserving the relationship between pixels of an image by learning its features using the small squares of input data. Presented in Fig. 2.1 is the process of CNN in image processing.

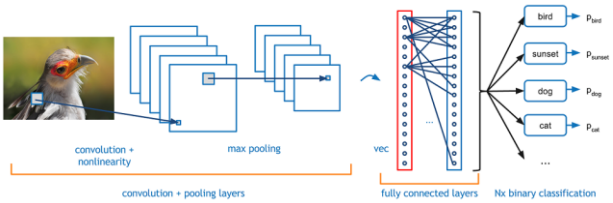


Figure 2.1. Convolutional Neural Network Diagram

B. Transfer Learning

Transfer learning is a machine learning method that uses pre-trained neural network such as inception-v3 wherein the feature extraction part with convolutional neural network was reused and the classification part was re-trained based on the dataset used. It can result to less training time and less computational cost and can still achieve accuracy [8].

C. Inception-v3

The inception model is a model used widely for image processing, especially for image recognition, which provides a high percentage of accuracy in reliance to the dataset in ImageNet. It was made up of several compositions such as convolutions, pooling and other layers fully connected to implement the idea of inception [9].

The version of the inception model, the Inception-v3, was one of the pre-trained models of inception under the idea of TensorFlow. It was considered as the latest version of the inception model. This model was trained using the datasets from ImageNet and found to be the inception model that can identify a great number of classes within the dataset tested [10]. Inception-v3 was divided into two parts: the feature extraction and the classification. The feature extraction consists of convolutional neural network, whereas the classification part consists of fully-connected layers and softmax layers.

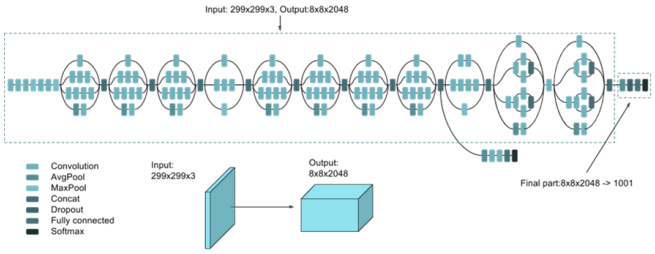


Figure 2.2. Inception Model's High-level Diagram

D. Training

The concept of transfer learning was used in the training process in the study and inception-v3 model was used as the pre-trained neural network. The convolutional and pooling layers of the inception-v3 are used to generate unique features from the image that is being trained.

As shown in Fig. 2.4, is the training process that was developed by the researchers.

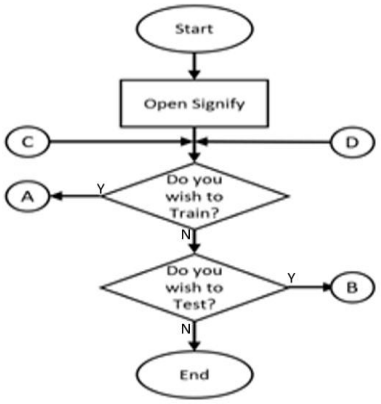


Figure 2.3. Main process of Signify

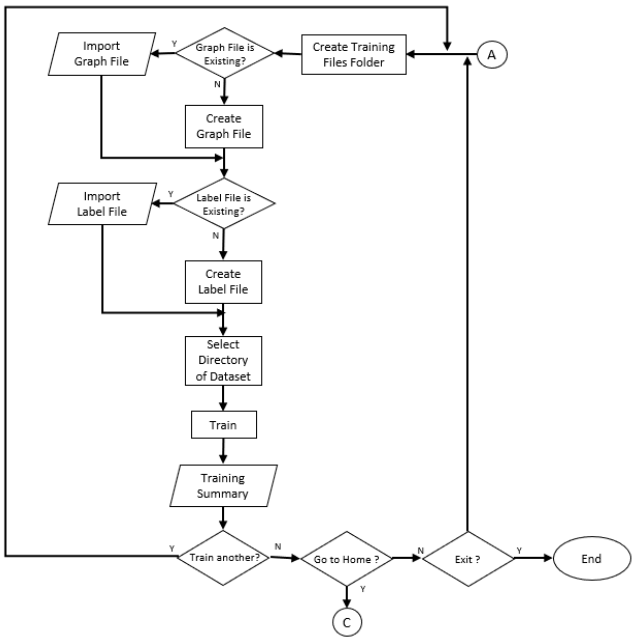


Figure 2.4. Training process of Signify

E. Testing

The fully connected layer of the convolutional neural network is assigned for the classification of an image.

Its main goal is to classify the image based on the features detected during the training process. As shown in Fig. 2.5, is the testing process of Signify.

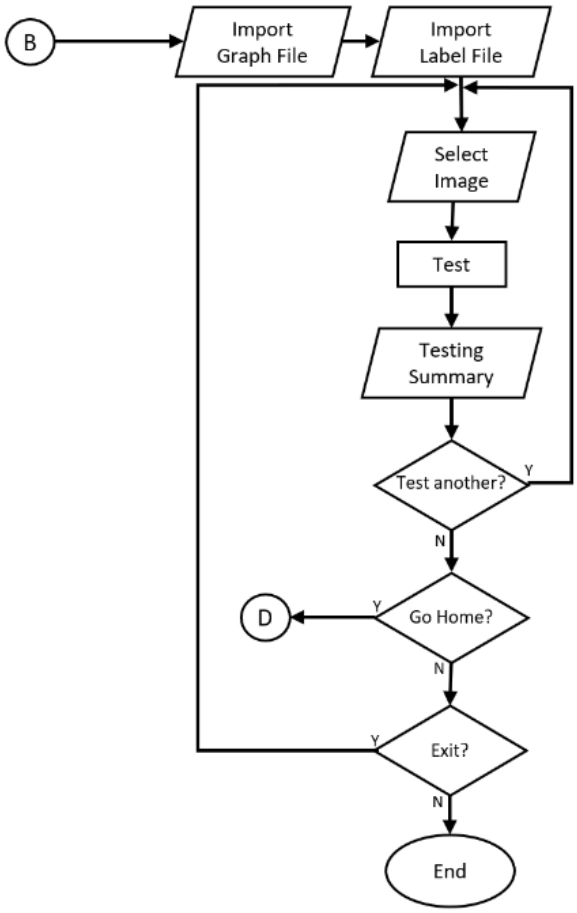


Figure 2.5. Testing process of Signify

F. Dataset

In this study a total of 400 genuine signatures of 4 people were used for training and 10 percent of it were used as validation set. As for the testing, mixture of genuine signature and forged signature were used. Some signatures were scanned and some were captured using phone camera. The researchers also included signatures with written name under it. As shown in Fig. 3.4, are some signature samples that were used in the study.

Figure 2.6. (a) Genuine signatures used for training

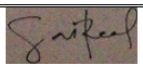
Figure 2.6. (b) Forged signatures used for testing

III. RESULTS AND ANALYSIS

The researchers tested 50 genuine signatures and computed the mean of the matching rate for it to be the standard percentage for classifying whether a signature is genuine or forged. Upon computing, 96.43% was the average of all the tested signatures therefore it was used as the standard matching rate in verification.

The summary of all the results of the training and the testing process of Signify proved that the number of datasets in the first place played a major concern in signature verification. As shown in Table 3.1, there was a huge difference between the results with one hundred and twenty (120) signatures and four hundred (400) signatures. The matching rate of the forged signature dropped drastically after the addition of signatures in the training set. It just proved that, as the number of datasets increased, the percentage of accuracy of the testing also increased.

Table 3.1. Summary results with different number of dataset

Image Tested		
With 120 Signatures trained (%)	cyril nj rodil - (69.92%)	cyril nj rodil - (99.05%)
Duration (seconds)	5.30	5.30
With 400 Signatures trained (%)	cyril nj rodil – (94.11%)	cyril nj rodil – (53.53%)
Duration (seconds)	5.50	44.58

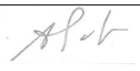
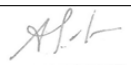
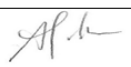
3.1 Factors affecting the results of Verification

After all the tests were done in signature verification using Signify, the following were the factors that affected the results of the verification process and provide the inconsistencies upon testing the program.

3.1.1 Use of Pencil and Colored Pen in Signing

The researchers proved that using different writing materials such as pencil or colored pens affected the verification. During the testing, all of the signatures tested resulted to either different name classification or low matching rate. From the researchers' assessment of the results and inconsistencies, Signify was a verification tool under the influence of Convolutional Neural Networks which provided results of signature verification with reference to each of the pixels of the pictures being tested. Signatures written using a regular black pen was compared to those written using a pencil and a colored pen, and presented differences when dealing with the pixels of the image. Images of signature written using a black pen provided more distinct characteristics of pixels than that of written using a pencil and other colored pen. As well as the shades of the color of the pen used in signing gave another set of results when verified using Signify. The processes under the idea of convolutional neural networks matched each of the pixels of the images to compare its resemblance with the trained set, and with the indistinctive characteristics of the pixels of the images of the signatures using pencil and colored pen, inconsistencies in verification was one of the results that might be encountered upon its usage. As shown in Table 3.2, one signature were classified as a signature of *"louie Andrew boo"* though it is a genuine signature of *"alexandra mae laylo"*. de

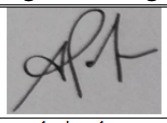
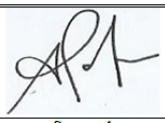
Table 3.2. Summary results of using pencil and colored pen

Image Tested	True Value	After Verification
	alexandra mae laylo - genuine	alexandra mae laylo (88.14%)
	alexandra mae laylo - genuine	louie andrew boo (54.44%)
	alexandra mae laylo - genuine	alexandra mae laylo (92.35%)

3.1.2 Ways of Dataset Acquisition

The ways of dataset acquisition provided inconsistencies and the results of the testing process of Signify. Shown in Table 3.3 was a sample signature tested that was captured image and a phone camera under the name of *"alexandra mae laylo"* as well as its testing that used the scanned image of that same signature. The matching rate of 98.64% and 95.15% provided not that much difference in terms of percentage but its accuracy in terms of classification under that name resulted different. One was considered genuine, and the other was considered forged.

Table 3.3. Test Summary with captured and scanned signature images

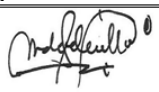
Signature Tested		
Way of acquisition	Captured using phone camera	Scanned
True Value	Genuine signature of alexandra mae laylo	Genuine signature of alexandra mae laylo
Classified as	alexandra mae laylo	alexandra mae laylo
Matching Rate	98.64%	95.15%
Classification based on standard matching rate	GENUINE	FORGED

Upon analysis, the researchers considered the ways of signature image acquisition as one of the factors that affected the verification of signatures tested using the Signify.

3.1.3 Size of the Signature Image

Shown in Table 3.4 was the test summary of the results in dependence with the size of the image. Presented in the table was the image of the signature tested with a size of 300x200 and provided different results with the image in the size of 449x201, which was a randomly picked image. The matching rate of the image with a uniform size of 300x200 provided 98.49% of accuracy that it was a genuine signature of *"mark daryl decillo"*. On the other hand, the signature with a random size of 449x201 presented 93.56% matching rate that was a forged signature of *"mark daryl decillo"*.

Table 3.3. Test Summary with Different Sizes of Signature Image

Signature Tested		
Image size	300x200	449x201
True Value	Genuine signature of mark daryl decillo	Genuine signature of mark daryl decillo
Classified as	mark daryl decillo	mark daryl decillo
Matching Rate	98.49%	93.56%
Classification based on standard matching rate	GENUINE	FORGED

The researchers considered also the size of the signature image, upon analysis, as one of the factors that affected the verification of signatures tested using Signify.

IV. CONCLUSION AND FUTURE WORKS

The researchers were able to accomplish the objectives of this study. The researchers were able to verify a certain signature and tell whether it is a forged or a genuine signature of the owner. Convolutional Neural Network (CNN) as the main algorithm was successfully used in developing the signature verification technique. The researchers were also able to create software that incorporates CNN for signature verification. The factors that affect the accuracy of the results were also identified in this study. Those factors include properties of the pen used, the size of the image being tested and the method of acquisition of the signature.

This study considerably showed the innovation for the old style of signature verification which was the manual testing and comparison of a tested signature among all the samples provided by the owner of the signature. The use of convolutional neural network proved that it was possible, and observably applicable. With that, the researchers believed that still, further enhancements to the design are still necessary.

Future researchers can increase the number of dataset to undergo training to have more accurate results. It is also recommended the addition of automatic signature exportation where the program will be the one to locate the signature in a certain scanned document, and a cropping tool.

ACKNOWLEDGMENT

The authors would like to impart their sincere gratitude and appreciation for the support and contribution of the following individuals to the completion of this research project: To God Almighty, for giving them life, enough knowledge and incomparable strength to surpass all the inconsistencies and troublesome situations along the stages of the completion of the project; To their family for their unconditional love, support, advise, and most especially, for their continuous prayers; To all their friends and loved ones who had been their inspiration, mood booster, resources and for giving them some tips as well as advises in making a good research project.

REFERENCES

1. Morton, A., Reid, W., Buntin, C., Brockly, M., O'Neill, J., Elliott, S., & Guest, R. (2015). *Signature forgery and the forger–an assessment of influence on handwritten signature production*. INFORMATION TECHNOLOGY IN INDUSTRY, 3(2), 54-58.
2. Sharma, Abhilash. (2015). *Biometric System- A Review*. International Journal of Computer Science and Information Technologies. 6. 4616-4619.
3. Azzopardi, G. (2008). *Offline handwritten signature verification using radial basis function neural networks*. George Azzopardi.
4. Kumar, S., & Shashwat, K. (2015). *A survey on handwritten signature verification techniques.* International Journal of Advance Research in Computer Science and Management Studies, 3(1), 182-186.
5. Gopichand G, S. G. (2019). *Digital Signature Verification Using Artificial Neural Networks*. International Journal of Recent Technology and Engineering, 7(6S), 467-472.
6. Mahanta, L. B., & Deka, A. (2013). *A study on handwritten signature*. International Journal of Computer Applications, 79(2).
7. ujjwalkarn. (2016, August 9). *quick-intro-neural-networks*. Retrieved from the data science blog: https://ujjwalkarn.me/2016/08/09/quick-intro-neural-networks/
8. Nithya Roopa S., P. M. (2018*). Speech Emotion Recognition using Deep Learning.* International Journal of Recent Technology and Engineering, 7(4S), 247-250.
9. *Advanced Guide to Inception v3 on Cloud TPU.* (2019, January 29). Retrieved from Google Cloud: https://cloud.google.com/tpu/docs/inception-v3-advanced
10. Islam, M. S., Foysal, F. A., Neehal, N., Karim, E., & Hossain, S. A. (2018). *InceptB: A CNN Based Classification Approach for Recognizing Traditional Bengali Games.* Procedia computer science, 143, 595-602.

AUTHORS PROFILE

Alexandra Mae C. Laylo is a graduate of Batangas State University with a bachelor's degree in Computer Engineering. She is a member of Institute of Computer Engineers of the Philippine, student edition (ICpEP.se).

Mark Daryl A. Decillo graduated with a degree of Bachelor of Science in Computer Engineering at Batangas State University, June 2019. He is a member of Institute of Computer Engineers of the Philippines, student edition.

Louie Andrew F. Boo received his B.S. Computer Engineering degree from Batangas State University, Philippines in 2019. His research interests include machine learning and computer programming.

Jeffrey S. Sarmiento received his Bachelor of Science in Computer Engineering degree in 2008. He obtained his Master of Science in Computer Engineering degree in 2016 and currently taking his Doctor of Engineering. No publication yet. He is a member of ICpEP, PSITE, ISITE, PSUCCESS, IAENG and HKBES.