FACULTY POSITION RECLASSIFICATION FOR SUCs
(DBM-CHED Joint Circular No. 3, series of 2022)

CERTIFICATION OF PERCENTAGE CONTRIBUTION

(Research Output with Multiple Authors)

Title of Research: **Computer Vision-Based Signature Forgery Detection System Using Deep Learning: A Supervised Learning Approach**

Type of Research Output: **Conference Paper (Scopus-Indexed, IEEE Paper)**

Instruction: Supply ALL the names of the authors involved in the research output and indicate the contribution of each author in percentage. Each author shall sign the conforme column if he/she agrees with the distibution. The conforme should be signed by all the authors in order to be considered. Please prepare a separate Certification for each output.

	Name	Current Affiliation	% Contribution	Conforme *(Sign if you agree with the % distribution)*
1	Ryan C. Reyes	TUP	14.28%	
2	Myriam J. Polinar	BISU	14.28%	
3	Richardson M. Dasalla	ISU	14.28%	
4	Godofredo S. Zapanta	PLP	14.28%	
5	Mark P. Melegrito	TUP	14.28%	
7	Renato R. Maaliw	SLSU	14.28%	
	**should have a total of 100%*		100%	

Prepared by:

RENATO R. MAALIW III, DIT
Faculty

Certified by:

NICANOR L. GUINTO, Ph.D
Research Director

2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT) | 978-1-6654-9781-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/CONECCT55679.2022.9865776

Computer Vision-Based Signature Forgery Detection System Using Deep Learning: A Supervised Learning Approach

Ryan C. Reyes
Department of Electrical Engineering
Technological University of the Philippines
Manila, Philippines
ryan_reyes@tup.edu.ph

Myriam J. Polinar
College of Engineering and Architecture
Bohol Island State University
Tagbilaran City, Bohol, Philippines
myriam.polinar@bisu.edu.ph

Richardson M. Dasalla
College of Computing Sciences
Ifugao State University
Ifugao, Philippines
dasallarichardson1979@gmail.com

Godofredo S. Zapanta Jr.
College of Engineering
Pamantasan ng Lungsod ng Pasig
Pasig, Philippines
zapanta_godofredojr@plpasig.edu.ph

Mark P. Melegrito
Department of Electronics Engineering
Technological University of the Philippines
Manila, Philippines
mark_melegrito@tup.edu.com

Renato R. Maaliw III
College of Engineering
Southern Luzon State, University
Lucban, Quezon, Philippines
rmaaliw@slsu.edu.ph

***Abstract*— Authentication is a crucial aspect of data security. It is one of the most important issues of our time. As technology advances, our interactions with machines are becoming increasingly automated. As a result, for a variety of security concerns, the demand for authentication is rapidly expanding. As a result, biometric-based authentication has become extremely popular. It has a significant edge over other approach. However, because different ways are utilized to verify people, this incidence is not a substitute for a problem. Signatures were one of the first commonly utilized biometric traits for identifying people. This paper describes a method for simplifying signature verification by preprocessing signatures. It also included a novel deep learning-based method for detecting faked signatures. With an accuracy of 85-95 %, the proposed method detects forgeries.**

Keywords—Authentication; Biometric; Verification; Pre-processing; Forged Signature

I. Introduction

Signature verification and fraud identification refer to the practice of electronically and immediately analyzing signs to identify if they are legitimate or not [1]. There are two main types of signature validation: fixed validation and dynamic verification. Dynamic, or online, validation occurs as a person creates his or her signature on an electronic tablet or similar item, while static, or offline, validation occurs after a paper signature is made. [2]. The signature in question is then compared against previous samples of that person's signature, resulting in the creation of the database [3]. When a written signature is discovered on a paper, the machine should digitize the samples for testing; nonetheless, a digital signature that has already been stored in file formats can be used for verification. A written sign is one of the most globally recognized personal attributes for confirming identity, whether in finance or business [4].

Offline signature verification can be accomplished in several methods, and most businesses today use at least one of them[5]. The system's static features, such as image processing methods for analyzing signature accuracy, are used in offline signatures [6]. A person's initial identification via a password is one of these. Other multimodal approaches that strictly authenticate a person's identification using the two biometric features are available [7].

The goal of this study is to provide an overview of Deep Learning Processes as well as a workflow. We begin with data collection and work our way through exploratory data analysis, data manipulation, data modeling, model validation, and user Deep Learning Inference. It will be tremendously advantageous to the community, such as banks, schools, and law companies if we can create an adequate deep learning technique from the dataset that can discern between fake and real signatures more precisely.

Students of information technology, computer science, and engineering, as well as IT professionals, IT corporations, law firms, banks, school systems, and future researchers, will be interested in the findings of this study. The data supplied will serve as a guide for their future research. They will be able to understand the benefits and drawbacks of various machine learning algorithms as early as now, thanks to this research. They will also identify the study's strengths and limitations. The study's findings will assist IT professionals in developing another efficient technique or framework linked to this study. Finally, the ideas presented in this study might serve as a catalyst for future research or as a method of validating the reliability of other associated breakthroughs.

The architecture of the YOLOv3 algorithm, the approach for recognizing original and faked signatures, model training, and testing using a custom data set will all be covered in the sections that follow. Section 3 deals with the experimental findings and discussions, whereas Section 4 deals with the conclusions and recommendations.

II. Methodology

The suggested technique is designed to identify the fabrication of signatures. The dataset that the system uses includes images from Kaggle [8]. The You-Only-Look-Once (YOLO) architecture is used to detect signature forgery. It is one of the Convolutional Neural Network architectures for real-

978-1-6654-9781-7/22/$31.00 ©2022 IEEE

time object detection. There are three main forms of YOLO. In this project, the most recent version, YOLO v3, is used. This is because when comparing YOLO v3 with YOLO v2 when speed isn't taken into account, YOLO v3 is more accurate than YOLO v2. The YOLO v3 is three times faster than the SSD (Single Shot Detector) and has the same accuracy [9]. Feature extraction and classification are the two steps of a typical Convolutional Neural Network [10]. The above-mentioned architecture is used to train the images for feature extraction. A darknet is a tool for learning. There are two types of predictions: genuine and fake. OpenCV and Keras are used for testing. In YOLO v3, both recognition and localization are available [11].

A. *Proposed Scheme*

This study proposes a novel method for signature recognition and forgery verification. The suggested system architecture is depicted in Fig. 1, in which the test signature is detected using deep learning with the supplied input training set. After that, counterfeit detection techniques based on deep learning are applied to this categorized image.

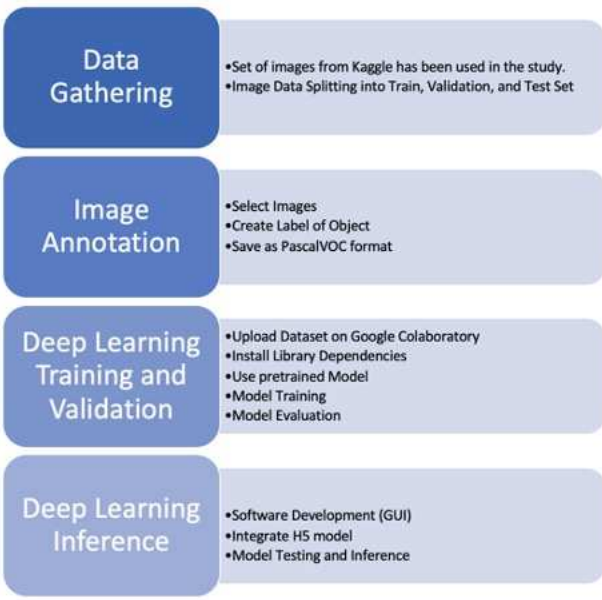

Fig. 1. System architecture for signature recognition and forgery detection.

B. *Preliminaries*

To compare and extract dependable characteristic discoveries from images, equipped photos must have similar forms, dimensions, and placement.

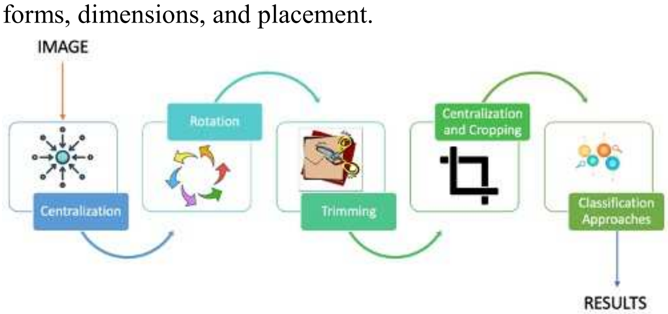

Fig. 2. Data pre-processing.

As a result, to obtain the requisite precision in feature detection, a variety of pre-processing methods are applied, as illustrated in Fig. 2.

C. *Dataset Gathering and Preparation*

The data for this study was carefully obtained from several internet sources, as shown in Fig. 3. Images of real and counterfeit signatures from various persons were collated and utilized as the dataset for the study. This categorization uses a total of 300 photos, 150 for real signatures and 150 for counterfeit signatures. The dataset was split into two sections, with 80% used for training and 20% for validation.

Fig. 3. Image Dataset for Original and Forged signatures.

D. *Image Annotation*

LabelImg is an open and free image labeling software. It's developed in Python and also has a graphical user interface depending on QT. It's a simple and quick approach to labeling several hundred photos for your next object detection project. In this case, counterfeit (Fig. 5) and genuine signatures (Fig. 4) were distinguished by annotating the photos with the appropriate categories.

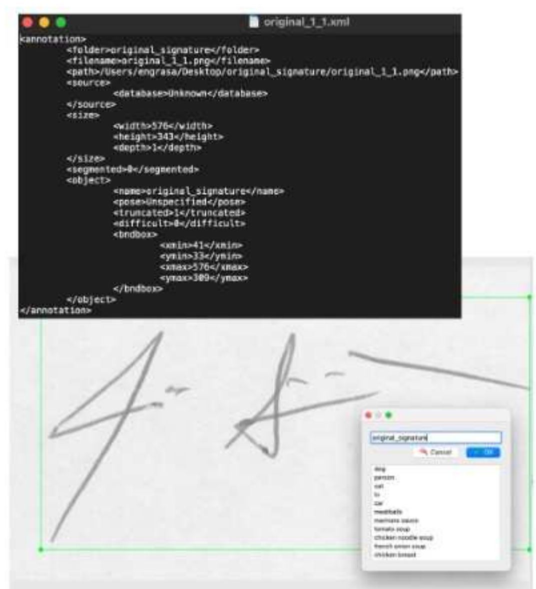

Fig. 4. Image annotation of the forged signature using labelImg.

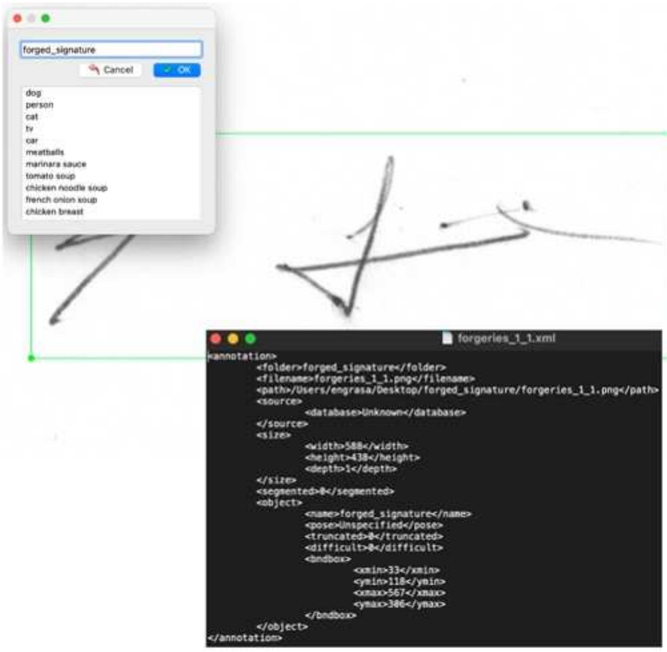

Fig. 5. Image annotation of the original signature using labelImg.

E. Algorithm for Transfer Learning

YOLOv3 is one of the fastest computer vision algorithms. As illustrated in Fig. 6, YOLOv3 divides the input picture into multiple pieces and applies a discrete convolutional neural network (CNN) to each segment to predict border boxes. CNN's capability to produce many projections at once is more effective. YOLOv3, or "you only look once," is one of the fastest object detecting methods. It divides an image into various sections using a CNN. This method is faster than classical feature extraction, which scans the entire image pixel by pixel for items. During object recognition, certain settings may be extremely noisy, busy, or perplexing, causing the item to be misread. YOLOv3 takes a localized solution to this problem, returning the picture region with the best reliability rating and the closest proximity to the detected item [16] – [26].

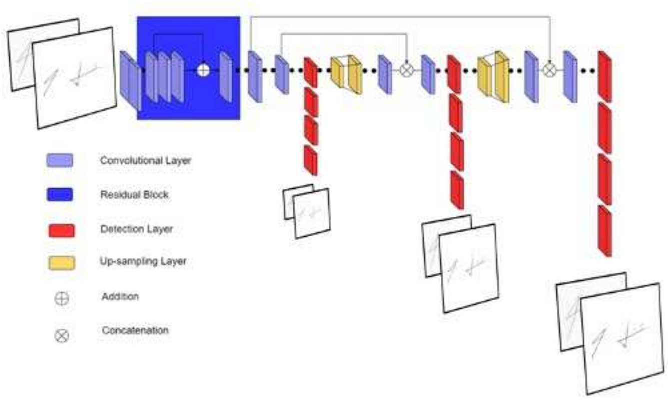

Fig. 6. YOLOv3 Architecture for signature forgery detection.

F. Deep Learning Evaluation

The mAP (Mean Average Probability) is used to detect model inference to verify that the fully trained algorithm for the task was chosen. The training set was evaluated with precision. It will produce data during the testing procedure. As the mAP increases, precision detection improves. The AP average is the mAP (mean average precision).

The mean average precision (mAP) (1) is the average efficiency (AP) of overall evaluations, where O is the number of items in the set and *APi* is the average accuracy (AP) for a dataset.

$$mAP = \frac{\sum_{i=1}^{O} AP_i}{O} \tag{1}$$

III. Results And Discussions

A. Training Model

Using the Keras-yolo3 package, which offers a lot of functionality for employing YOLOv3 models, you can do things like object identification, transfer learning, and training new models from start.

In this phase, the pre-trained model was used to identify signature fraud on an unseen picture. This feature is included in the repository in a single Python file called "pretrained-yolov3.h5.1." This script creates a model using pre-trained weights, then uses that model to detect objects and generate a model. It also makes use of OpenCV.

Rather than using this software directly, the components were utilized to create scripts that prepared and saved a Keras YOLOv3 model and then loaded the model to produce a photo prediction. The YOLO v3 Training and Validation Loss result and details are shown in Fig. 7.

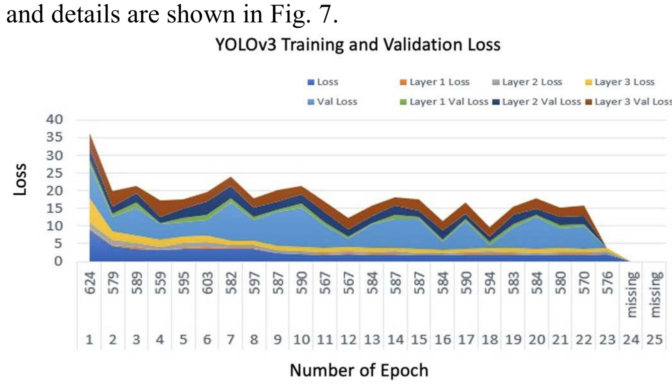

Fig. 7. YOLO v3 Training and Validation Loss.

B. Validation Model

On a test data set, a trained model was evaluated in this phase. This makes it possible for a trained model to generalize. Our trained models produced three models that were more than 95% accurate. The trained models' greatest accuracy was 98.35 %, while the lowest was 22.15 % as shown in Fig. 8.

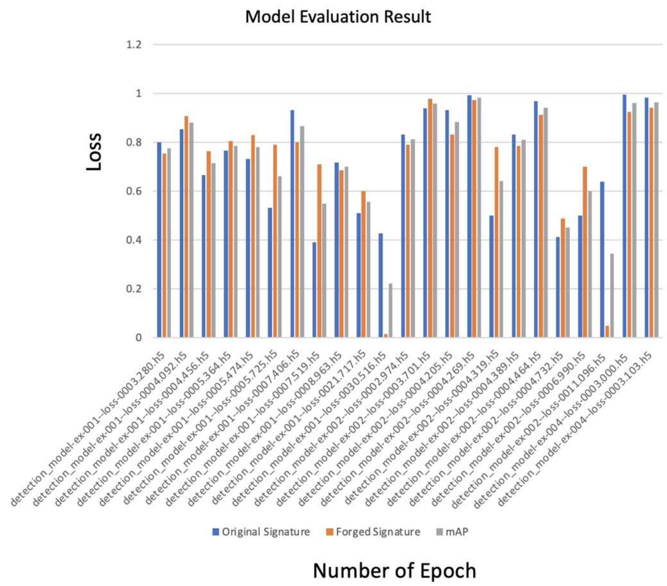

Fig. 8. Model Evaluation Result (mAP)

C. Deep Learning Inference

The deep learning inference of a signature forgery detection system is shown in Fig. 9. The user has three options for uploading a signature for verification, specifying whether it is forged or not.

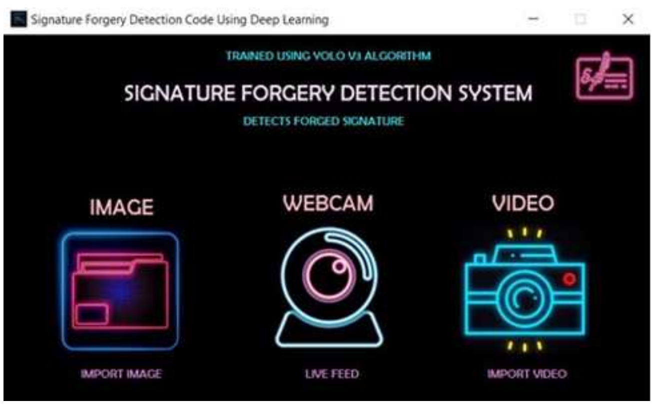

Fig. 9. Deep Learning Inference of Signature Forgery Detection System

If the user chooses the picture option, the file must be in the jpeg or png format, or else the system will refuse it. Fig. 10 is an example of what can be done using the image option.

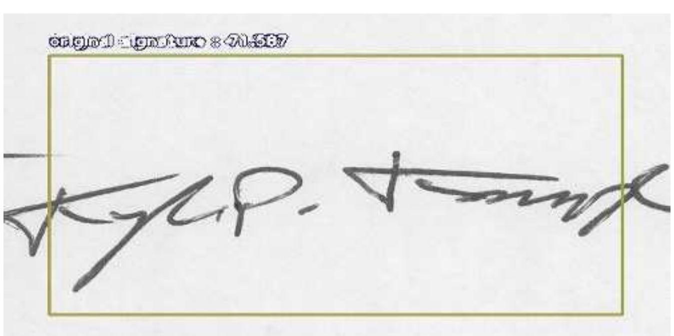

Fig. 10. Detected original signature using image option.

If the user chooses the webcam option, the user's computer's camera will automatically open. The system will record a video of the user signing something. This option produces the image below as an example output shown in Fig. 11 and Fig. 12.

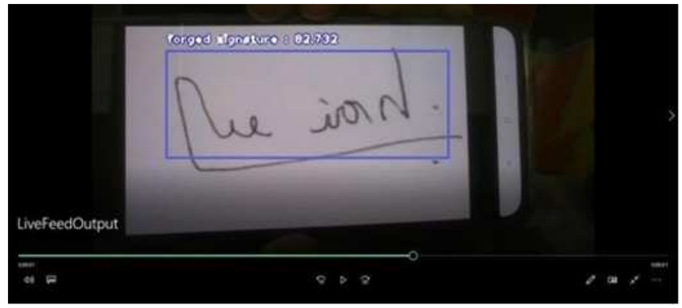

Fig. 11. Detected forge signature using webcam option.

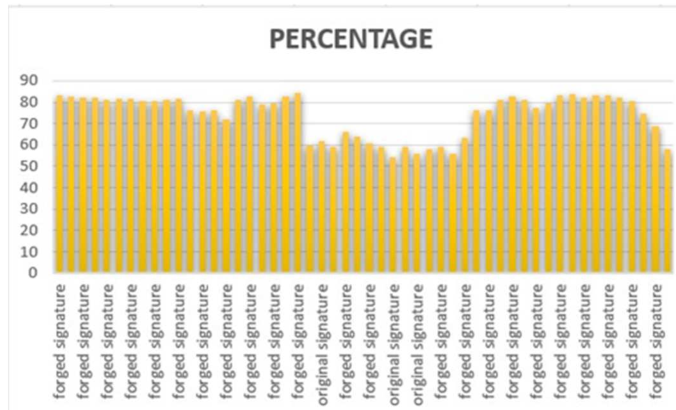

Fig. 12. Live feed testing result.

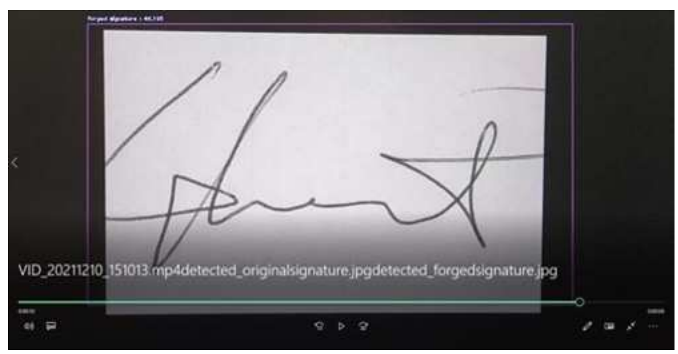

Fig. 13. Detected forged signature using video option.

If the user chooses the video option, the video must be in avi or mp4 format; otherwise, the system will refuse it. The output of the system while using the video module is shown in Fig. 13 and Fig. 14.

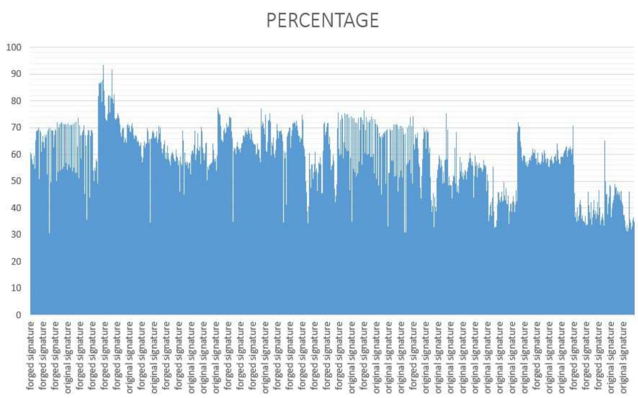

Fig. 14. Video testing result.

IV. Conclusion and Recommendation

To improve annotation process performance, a poorly trained detector is sufficient. Because it filters poor prediction samples, the detector's accuracy must be improved by lowering the probability threshold.

The installation of a YOLO network for signature forgery detection produces improved results even when YOLO v3 is trained on an image captured with a visible spectrum camera.

The YOLO v3 was retrained, resulting in improved signature forged detection system performance and the ability to automatically recognize forged signatures in low-resolution situations.

The fundamental goal of this research is to improve prediction approaches using various combinations of deep learning techniques. Furthermore, new feature selection methods can be created in order to acquire a larger perception of the important features and thus increase the effectiveness of signature forged detection systems.

Acknowledgment

The authors thank all of the colleges, institutions, and universities with which they are associated.

References

[1] J. Linden, F. Taroni, R. Marquis and S. Bozza, "Bayesian multivariate models for case assessment in dynamic signature cases", *Forensic Science International*, vol. 318, p. 110611, 2021. doi: 10.1016/j.forsciint.2020.110611.

[2] P. Patil and B. Patil, "A Review - Signature Verification System Using Deep Learning: A Challenging Problem", *International Journal of Scientific Research in Science and Technology*, pp. 295-298, 2021. doi: 10.32628/ijsrset207632.

[3] N. Goyal, M. Ram and A. Kumar, "Signature analysis of a combinatory system", *Materials Today: Proceedings*, vol. 46, pp. 11263-11266, 2021. doi: 10.1016/j.matpr.2021.03.231.

[4] W. Khoh, Y. Pang, A. Teoh and S. Ooi, "In-air hand gesture signature using transfer learning and its forgery attack", *Applied Soft Computing*, vol. 113, p. 108033, 2021. doi: 10.1016/j.asoc.2021.108033.

[5] J. Poddar, V. Parikh and S. Bharti, "Offline Signature Recognition and Forgery Detection using Deep Learning", *Procedia Computer Science*, vol. 170, pp. 610-617, 2020. doi: 10.1016/j.procs.2020.03.133.

[6] A. Zenati, W. Ouarda and A. Alimi, "SSDIS-BEM: A New Signature Steganography Document Image System based on Beta Elliptic Modeling", *Engineering Science and Technology, an International Journal*, vol. 23, no. 3, pp. 470-482, 2020. doi: 10.1016/j.jestch.2019.09.002.

[7] N. Yousefnezhad, A. Malhi and K. Främling, "Security in product lifecycle of IoT devices: A survey", *Journal of Network and Computer Applications*, vol. 171, p. 102779, 2020. doi: 10.1016/j.jnca.2020.102779.

[8] I. Adeyanju, O. Bello and M. Adegboye, "Machine learning methods for sign language recognition: A critical review and analysis", *Intelligent Systems with Applications*, vol. 12, p. 200056, 2021. doi: 10.1016/j.iswa.2021.200056.

[9] J. Xiao, "exYOLO: A small object detector based on YOLOv3 Object Detector", *Procedia Computer Science*, vol. 188, pp. 18-25, 2021. doi: 10.1016/j.procs.2021.05.048.

[10] P. Jain, P. Gajbhiye, R. Tripathy and U. Acharya, "A two-stage deep CNN architecture for the classification of low-risk and high-risk hypertension classes using multi-lead ECG signals", *Informatics in Medicine Unlocked*, vol. 21, p. 100479, 2020. doi: 10.1016/j.imu.2020.100479.

[11] Ali et al., "A deep learning framework for quality assessment and restoration in video endoscopy", *Medical Image Analysis*, vol. 68, p. 101900, 2021. doi: 10.1016/j.media.2020.101900.

[12] Poddar, J., Parikh, V., & Bharti, S. K. (2020). Offline Signature Recognition and Forgery Detection using Deep Learning. Procedia Computer Science, 170, 610–617. doi: 10.1016/j.procs.2020.03.133

[13] Mshir, S., & Kaya, M. (2020). Signature Recognition Using Machine Learning. 2020 8th International Symposium on Digital Forensics and Security (ISDFS). doi:10.1109/isdfs49300.2020.9116199

[14] Ghanim, T. M., & Nabil, A. M. (2018). Offline Signature Verification and Forgery Detection Approach. 2018 13th International Conference on Computer Engineering and Systems (ICCES). doi:10.1109/icces.2018.8639420

[15] Lakshmi, K. V., & Nayak, S. (2013). Off-line signature verification using Neural Networks. 2013 3rd IEEE International Advance Computing Conference (IACC). doi:10.1109/iadcc.2013.6514374

[16] M. J. Alhaddad, D. Mohamad, and A. M. Ahsan, "Online Signature Verification Using Probabilistic Modeling and Neural Network," in Engineering and Technology (S-CET), 2012 Spring Congress on, 2012, pp. 1-5.

[17] J. Redmon and A. Farhadi, "YOLOv3: An Incremental Improvement", *arXiv*, 2018.

[18] J. Hipolito, A. Sarraga Alon, R. Amorado, M. Fernando and P. De Chavez, "Detection of Underwater Marine Plastic Debris Using an Augmented Low Sample Size Dataset for Machine Vision System: A Deep Transfer Learning Approach", *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, 2021. doi: 10.1109/scored53546.2021.9652703.

[19] M. Pita, A. Alon, P. Melo, R. Hernandez and A. Magboo, "Indoor Human Fall Detection Using Data Augmentation-Assisted Transfer Learning in an Aging Population for Smart Homecare: A Deep Convolutional Neural Network Approach", *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, 2021. doi: 10.1109/scored53546.2021.9652769.

[20] A. Alon, "COINIC-PH: A PHILIPPINE NEW GENERATION SERIES OF COIN INTELLIGENT CLASSIFICATION INFERENCE APPROACH FOR VISUALLY IMPAIRED", *Journal of Engineering and Applied Sciences*, vol. 16, no. 19, 2021.

[21] J. Macalisang, A. Alon, M. Jardiniano, D. Evangelista, J. Castro and M. Tria, "Drive-Awake: A YOLOv3 Machine Vision Inference Approach of Eyes Closure for Drowsy Driving Detection", *2021 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, 2021. doi: 10.1109/iicaiet51634.2021.9573811.

[22] R. Sevilla, A. Alon, M. Melegrito, R. Reyes, B. Bastes and R. Cimagala, "Mask-Vision: A Machine Vision-Based Inference System of Face Mask Detection for Monitoring Health Protocol Safety", *2021 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, 2021. doi: 10.1109/iicaiet51634.2021.9573664.

[23] M. Melegrito, A. Alon, S. Militante, Y. Austria, M. Polinar and M. Mirabueno, "Abandoned-Cart-Vision: Abandoned Cart Detection Using a Deep Object Detection Approach in a Shopping Parking Space", *2021 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, 2021. doi: 10.1109/iicaiet51634.2021.9573963.

[24] A. Alon, J. Macalisang, R. Reyes, R. Sevilla and G. Belga, "Watercraft-Net: A Deep Inference Vision Approach of Watercraft Detection for Maritime Surveillance System Using Optical Aerial Images", *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 2020. doi: 10.1109/icetas51660.2020.9484279.

[25] N. Merencilla, A. Sarraga Alon, G. Fernando, E. Cepe and D. Malunao, "Shark-EYE: A Deep Inference Convolutional Neural Network of Shark Detection for Underwater Diving Surveillance", *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 2021. doi: 10.1109/iccike51210.2021.9410715.

[26] A. Alon, R. Dellosa, N. Pilueta, H. Grimaldo and E. Manansala, "EyeBill-PH: A Machine Vision of Assistive Philippine Bill Recognition Device for Visually Impaired", *2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, 2020. doi: 10.1109/icsgrc49013.2020.9232557

2022 IEEE International Conference on Electronics, Computing and Communication Technologies, CONECCT 2022 • 2022 • 2022 IEEE International Conference on Electronics, Computing and Communication Technologies, CONECCT 2022 • Bangalore • 8 July 2022through 10 July 2022 • Code 182416

Document type
Conference Paper
Source type
Conference Proceedings
ISBN
978-166549781-7
DOI
10.1109/CONECCT55679.2022.9865776
View more

Computer Vision-Based Signature Forgery Detection System Using Deep Learning: A Supervised Learning Approach

Reyes, Ryan C.[a]; Polinar, Myriam J.[b]; Dasalla, Richardson M.[c]; Zapanta, Godofredo S.[d]; Melegrito, Mark P.[a]; Maaliw, Renato R.[e]
Save all to author list

[a] Technological University of the Philippines, Department of Electrical Engineering, Manila, Philippines
[b] Bohol Island State University, College of Engineering and Architecture, Tagbilaran City, Philippines
[c] Ifugao State University, College of Computing Sciences, Ifugao, Philippines
[d] Pamantasan Ng Lungsod Ng Pasig, College of Engineering, Pasig, Philippines
View additional affiliations

Abstract

Authentication is a crucial aspect of data security. It is one of the most important issues of our time. As technology advances, our interactions with machines are becoming increasingly automated. As a result, for a variety of security concerns, the demand for authentication is rapidly expanding. As a result, biometric-based authentication has become extremely popular. It has a significant edge over other approach. However, because different ways are utilized to verify people, this incidence is not a substitute for a problem. Signatures were one of the first commonly utilized biometric traits for identifying people. This paper describes a method for simplifying signature verification by preprocessing signatures. It also included a novel deep learning-based method for detecting faked signatures. With an accuracy of 85-95 %, the proposed method detects forgeries. © 2022 IEEE.

Author keywords

Authentication; Biometric; Forged Signature; Pre-processing; Verification

SciVal Topics
Metrics

Indexed keywords

SciVal Topics

Metrics

References (26)

1 Linden, J., Taroni, F., Marquis, R., Bozza, S.
Bayesian multivariate models for case assessment in dynamic signature cases
(Open Access)
(2021) *Forensic Science International*, 318, art. no. 110611. Cited 4 times.
www.elsevier.com/locate/forsciint
doi: 10.1016/j.forsciint.2020.110611
View at Publisher

2 Patil, P., Patil, B.
A Review-Signature Verification System Using Deep Learning: A Challenging Problem
(2021) *International Journal of Scientific Research in Science and Technology*, pp. 295-298. Cited 2 times.

SciVal Topics
Metrics

Computer Vision-Based Signature Forgery Detection System Using Deep Learning: A Supervised Learning Approach

Publisher: IEEE Cite This PDF

Ryan C. Reyes ; Myriam J. Polinar ; Richardson M. Dasalla ; Godofredo S. Zapanta ; Mark P. Melegrito ; Renato R. Maaliw **All Authors**

Abstract:
Authentication is a crucial aspect of data security. It is one of the most important issues of our time. As technology advances, our interactions with machines are becoming increasingly automated. As a result, for a variety of security concerns, the demand for authentication is rapidly expanding. As a result, biometric-based authentication has become extremely popular. It has a significant edge over other approach. However, because different ways are utilized to verify people, this incidence is not a substitute for a problem. Signatures were one of the first commonly utilized biometric traits for identifying people. This paper describes a method for simplifying signature verification by preprocessing signatures. It also included a novel deep learning-based method for detecting faked signatures. With an accuracy of 85-95 %, the proposed method detects forgeries.

Published in: 2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)

Date of Conference: 08-10 July 2022

Date Added to IEEE *Xplore*: 30 August 2022

ISBN Information:

Electronic ISBN:978-1-6654-9781-7

Print on Demand(PoD) ISBN:978-1-6654-9782-4

ISSN Information:

Electronic ISSN: 2766-2101

Print on Demand(PoD) ISSN: 2334-0940

INSPEC Accession Number: 22011154

DOI: 10.1109/CONECCT55679.2022.9865776

Publisher: IEEE

Conference Location: Bangalore, India

I. Introduction

Signature verification and fraud identification refer to the practice of electronically and immediately analyzing signs to identify if they are legitimate or not [1]. There are two main types of signature validation: fixed validation and dynamic verification. Dynamic, or online, validation occurs as a person creates his or her signature on an electronic tablet or similar item, while static, or offline, validation occurs after a paper Sign in to Continue Reading re in question is then compared against previous samples of that person's signature, res se [3]. When a written signature is discovered on a paper, the machine should digitize the samples for testing; nonetheless, a digital signature that has already been stored in file formats can be used for verification. A written sign is one of the most globally recognized personal

Authors

Figures

References

Keywords

Metrics