OFFLINE SIGNATURE VERIFICATION SYSTEM USING SIAMESE NEURAL NETWORK

Cajucson, Laylanie C.

Dalumpines, Sophia J.

Delos Reyes, Christine G.

Flor, Lea O.

Ugay, Mark Zaired D.

In Partial Fulfillment of the Requirements

for the Subject Course

Software Engineering 2

July 2023

ABSTRACT

When authenticating personal papers including approvals, bank checks, certificates, credit card transactions, passports, visas, letters, bonds, and contracts, a person's handwritten signature serves as a physical representation of their identity. In academic, administrative, financial, legal, and other professional environments, signatures are crucial in preventing attempts to falsify documents. Having said that, forging continues to be a problem today. Because of this, signature verification is crucial in everyday transactions. This research is an attempt to create a method for offline signature verification. The researchers make use of the Siamese Neural Network-centered system model. This study is centered on using a Siamese Neural Network (SNN) in developing an offline signature verification system. The system is a comprehensive software solution designed to authenticate handwritten signatures without relying on an internet connection. This system utilizes machine learning techniques to analyze and compare signature samples against a reference database, offering a reliable and efficient method for signature verification.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

THE PROBLEM AND ITS SETTING

This chapter seeks to provide the background and significance of the study. The objectives are listed, as well as the scope and limitations. This chapter will provide an overview of the research and a brief description of the concepts discussed in the study.

Background of the Study

When authenticating personal papers including approvals, bank checks, certificates, credit card transactions, passports, visas, letters, bonds, and contracts, a person's handwritten signature serves as a physical representation of their identity. In academic, administrative, financial, legal, and other professional environments, signatures are crucial in preventing attempts to falsify documents. Having said that, forging continues to be a problem today [1]. Because of this, signature verification is crucial in everyday transactions.

Signature verification is used in multiple sectors simultaneously almost every minute of every day. From validating IDs in record-keeping institutions, passports in airports, and checks in banks, to even investigating and solving legal cases. A signature verification system must have the following key features to be successful in its various applications: efficiency, speed, and accuracy of the output.

Depending on the format that the system accepts, there are two different methods of signature verification: online and offline. [2] Over the past few decades, a variety of cutting-edge techniques have been proposed and evaluated in the context of offline signature verification systems. [3] This research, too, is an attempt to create a method for offline signature verification. However, the researchers make use of a Siamese Neural Network-centered system model.

Project Objectives

The objectives of the study *Offline Signature Verification System Using Siamese Neural Network* are as follows:

- To develop an offline system that would verify the authenticity of a signature.
- To deploy a system that would make validating signatures easier and more efficient.
- To use Siamese Neural Network for the system model.
- To produce an output having an accuracy rate of at least 80% on authenticity and forgery detection.
- To test the model.
- To validate and evaluate the web application using ISO 25010.

Significance of the Study

Banks, record-keeping offices, and other billing departments of enterprises and establishments are potential beneficiaries of a signature verification system due to the growing need for a failsafe system to ensure the highest level of security from signature forgeries. The study's output system can also be used in smaller sectors, such as barangays, to create a more efficient and secure document processing system. Finally, the system could eventually eliminate the need for manually verifying signatures, closing out the possibility of human error.

Scope and Limitations

This study's output system operates offline. The model used by the researchers to determine if the input signature is genuine or fraudulent will be a Siamese Neural Network. Once the user has input two images of the signature, the system will proceed to perform its most

important function. The original signature in the first image must serve as the basis for comparison, and the signature in the second image is the one to be verified. Subsequently, the results will vary based on the image quality.

Chapter 2

CONCEPTUAL FRAMEWORK

The literature and studies cited in this chapter tackle the different concepts, understanding, ideas, and different development related to the study. Chapter II also presents the framework for the study that comprises the main focus of the research. Those that were included in this chapter help in familiarizing information that is relevant to the current study.

Conceptual Model of the Study

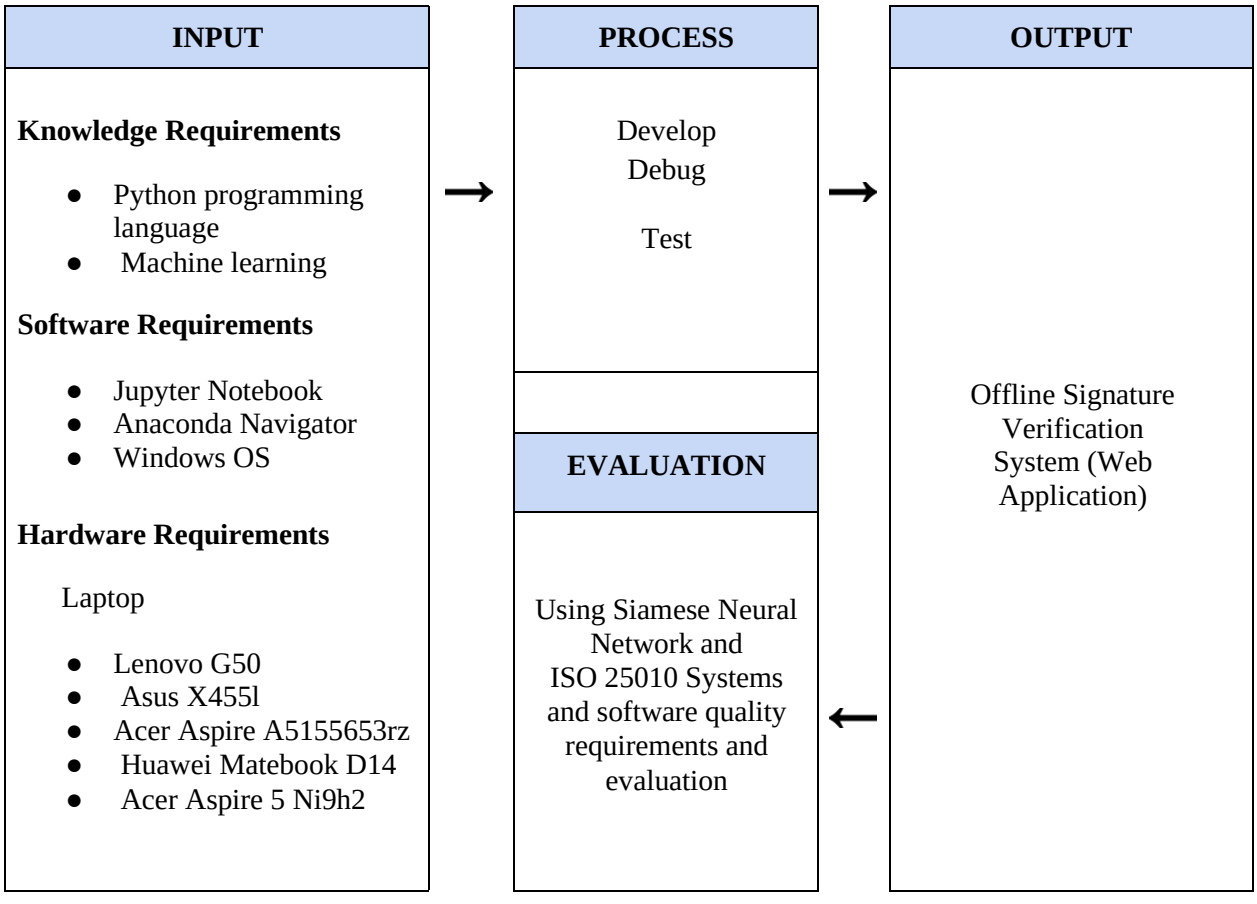

Figure 1. *Conceptual Model of the Web Application*

Input. The input block contains the knowledge, software, and hardware requirements required to create and develop the web application of offline signature verification. The knowledge requirements are the information that the researchers need to understand to have a good familiarity with the study being done. The software requirements are the needed application programs, frameworks, and operating systems to create the web application since this web application will need most of these for it to be developed properly. The hardware requirements are the tools needed to create the mobile application on and for the actual demonstration of it.

Process. The process diagram block includes developing, debugging, and testing activities to create the web application for offline signature verification. Ing. The developers should examine the background problem, create the features for an application, and start coding during the development stage. The developers inspect the program during the debugging stage to make sure there are no issues or errors. And lastly, in testing, a developed application must also go through several tests to ensure that it is functioning as intended and free from faults and problems.

Output. The output diagram block displays the developed web application for offline signature verification.

Evaluation. The performance of the Offline Signature System will be assessed using the test set by comparing the predicted similarity scores from the network with the true labels of the test set using the Siamese Neural Network.

Related Literature

Given the volume of labor required and the number of times it has been done, offline signature verification remains one of the most difficult tasks in the field of forgery detection. Various forgeries, including simple, random, and skilled forgeries, complicate the job. Handcrafted features such as block codes and wavelets have been used in previous approaches to solving the problem. However, in more modern offline systems, from the scanned signature images, only the pixel images must be analyzed, making the characteristics used for signature verification much relatively simpler [4,5]. Because there are no consistent dynamic characteristics, offline processing remains difficult. Many aspects of the signature, such as its starting and ending positions, angle of inclination, width, height, and comparative spacing between the letters, vary even between the same person. [6,7]

This is where the various techniques that have been discovered and refined over time come into play. Among these methods are neural networks. Because of their ability to detect classes of input signatures through parallel processing of neurons, they are useful for general pattern-matching applications and signature verification. One of the most advanced face detection and signature verification technologies currently in use is the Convolutional Neural Network (CNN). [8, 9] The Siamese network is made up of twin convolutional neural networks with similar biases and weights. It is distinguished by the use of two similar and parallel neural networks that have been successfully applied to real-time applications. [10,11]

In 2018, Kumari and Rana presented an intelligent algorithm for extracting information from signature images to distinguish between authentic and forged signatures. They combined

six CEDAR (Center of Excellence for Document Analysis) database elements, including the Area, Average Object Area, Euler, and Mean, to produce the best results. [12]

Abdalhaleem, Barakat, and El-Sana conducted research in 2018 on evaluating a Siamese Neural Network-based system that aims to divide a manuscript into portions and organize them based on stylistic similarity. They were able to yield a result that displayed how well the Siamese network classified the input paragraph's comparison dissimilarity. [13]

Furthermore, W. Shaikh, Nishad, Rai, and S. Shaikh demonstrated a signature verification system based on Augmented Reality in 2021. Key geometric factors that can be used to distinguish between different people's signatures were extracted from pre-processed images in their study. [14]

Chapter 3

METHODOLOGY

This chapter presents the project design, software design, database design, project development, and database setup. Also included in this section are the procedures that the researchers will use to complete the study's system.

Project Design

This study focuses on the development of an Offline Signature Verification System by leveraging the Siamese Neural Network (SNN). The training process of the SNN model was carried out through the utilization of Jupyter Notebook and Google Colaboratory. The signatures of 22 individuals were used as a dataset to train the model. To facilitate the deployment of the model, PyQT was employed.

System Design

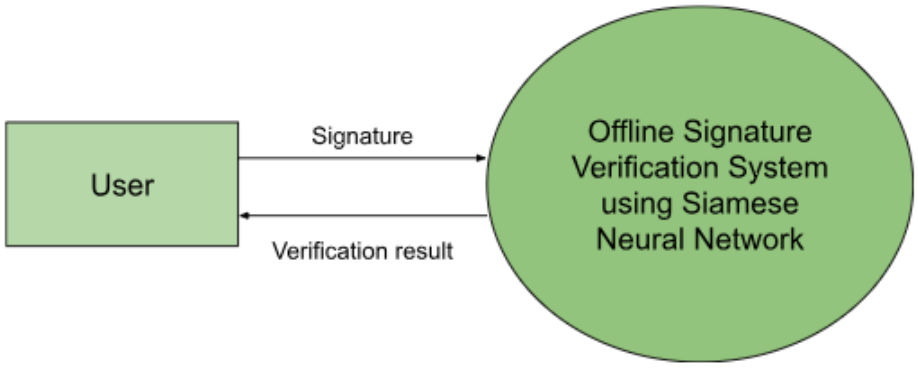

Figure 2. *Context Diagram for the Offline Signature Verification System using Siamese Neural Network*

The general system process is depicted here in this diagram. Figure 2 shows that the user will input two signatures – one genuine and another intended for verification – to be verified using the offline signature verification system. The system utilizes Siamese Neural Network to ascertain

the authenticity of the signature. Subsequently, the user will then be informed whether the submitted signature is genuine or forged.

Software Design

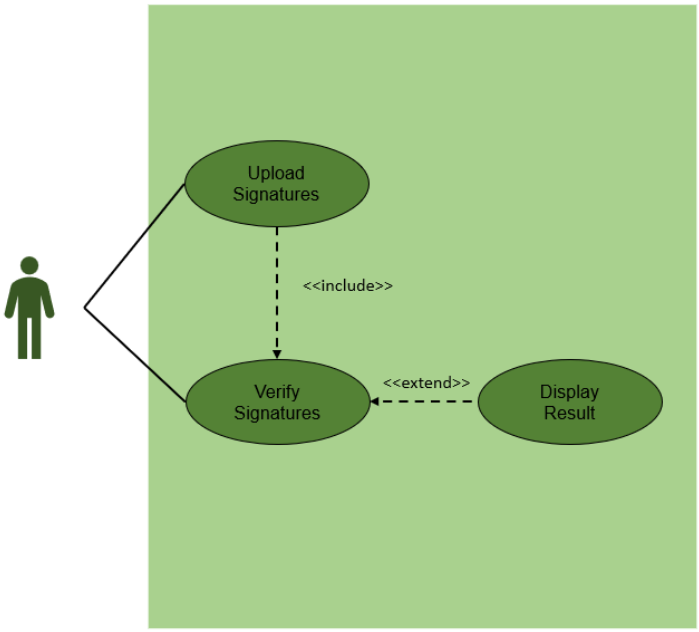

Figure 3. *Use Case Diagram for Offline Signature Verification System using Siamese Neural Network*

The Use Case Diagram depicts the expected interaction from both the external actors, the user, and the system. Additionally, the diagram also shows the main functionality of the system.

Figure 3 depicts the following features and cases for the Offline Signature Verification System using Siamese Neural Network:

- Upload Signature: The user can upload two images of the signature to the website, which will be used as the reference signature for verification.
- Verify Signature: The uploaded images will then be verified by the website. The system will use the Siamese Neural Network to compare it to the reference signature and provide a similarity score.

Project Development

This part presents the progress of the project and the details of the process that the researcher will use to develop the system. The process is composed of eight phases, which are: requirements, design, development, testing, deployment, review, delivery, and feedback. The project procedure begins with the discovery of existing studies about building systems. This study was selected out of the three projects the researchers proposed. The researchers then gathered more information that supports this study and created diagrams that would help visualize the structure of the system. To develop the project, Agile Software Development is used. The researchers aim to successfully build and improve the project until the expected requirements and accuracy are met. The users will take part in this project by providing feedback and ideas on how to improve the performance of the system.

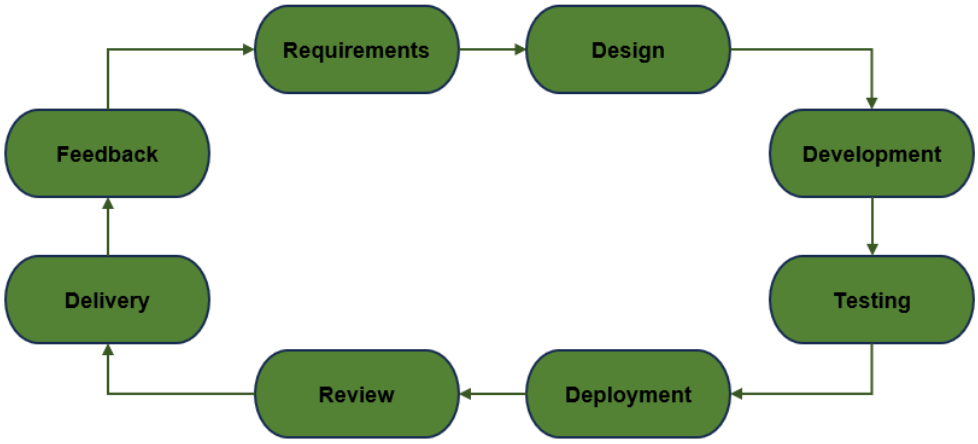

Figure 4. *Agile Software Development*

Requirements. The process begins by acquiring the needed requirements that the user will need to use the verification system, such as devices, features, and so on. The goal is to concentrate on the most frequently used and in-demand aspects by users. The least-used details can be used if they have been addressed after the execution of the system, which consists of basic features.

Design. After addressing requirements, the next process will be designing the software using two different operations, which are interface and architectural. The researchers select the best option for the framework, algorithm, and programming language, to provide a highly accurate result and the best experience for the user. There will be a preliminary model that will serve as the visual presentation of the user interface (UI), which will help illustrate the architectural design of the verification system. In addition, the data, such as signatures and user information, will be stored on the dataset which also has its design.

Development. The researcher will perform the coding and software design in the development stage. This is where the system is created with the support of approved requirements and prototypes from the previous phase. This process is the longest to perform, as the researchers are developing and designing the main foundation of the subject. This development phase will be subject to an end when the program is already successfully designed according to accepted conceptual plans and the errors are corrected.

Testing. A testing phase will be conducted before the verification system is delivered to the server. This process includes a pre-evaluation to determine if the system is error-free and has already been debugged successfully. There will also be numerous tests and experiments to check if the system performs consistently and provides accurate results.

Deployment. Following the testing stage, the system will be deployed for beta testing on real users. Through this deployment, the researchers will collect initial feedback from the beta users, both positive and negative, on how to further improve the system. It will also be the stage where fixes that were discovered during the beta testing will be addressed.

Review. Before proceeding with commercialization, the system product will go through a reevaluation process. This is done to ensure that the system is fully functional and ready for commercial use.

Delivery. The system product is now ready for market use following the reevaluation phase.

Feedback. When the product is in commercial use, users will provide varying feedback based on their preferences and usage experience. User feedback will be collected and incorporated into the development of future versions.

Database Setup

Operation and Testing Procedure

A Siamese Neural Network will be utilized as a measure of whether the signature is forged or authentic. The following procedure will be followed in order to operate the Offline Signature Verification System properly:

1. Run the program of the Offline Signature Verification System on a pc or laptop.
2. Provide signatures to be compared to the reference signatures stored by the administrator.

Table 1.

Operating and Testing Procedure of the Offline Signature Verification System using Siamese Neural Network (User Interface)

System Function	Procedure	Expected Output
1. Signature uploads	A system for obtaining signature samples from users by uploading an image.	- One genuine scanned signature and one scanned image intended to be verified (JPEG, PNG, BMP).
2. Preprocessing	A module in preparation of signature samples for extraction and analysis including resizing, enhancement, and normalization. It is used to improve the quality of the signature images and make them suitable for extraction. STEPS: ● To make all signature images the same size, resize them. ● Cropping an image removes any background noise or irrelevant information. ● Image enhancement: to make the signature more visible and easier to extract features. ● Process of ensuring that all signature images have the same lighting, contrast, and	- The signature must be: ● Cleaned ● Normal ● Enhanced -Make the images as similar as possible to all users.

	color. ● Process of converting an image to a binary image. ● Process of correcting any skewness in the signature.	
3. Extraction of data	A module for extracting relevant features from the preprocessed signature images, including curvature, slant, and width.	Extract features that are unique to each user's signature and are resistant to variations in signature images.
4. Comparing of signatures	A module for determining the difference score between the two signatures using Contrastive Loss and Euclidean Distance,	- Compare the input signature to the user's template signature. - Difference score of both signatures will be used to determine whether the input signature is genuine or forged.
5. Decision-making	A module for making a decision about the authenticity of a signature based on the output of the comparison module.	Threshold-based decision-making method: above 0.8 is considered a genuine signature. If below 0.8, the signature is considered forged.
6. Result Output	A module for showing the results of the verification process to the user.	

Evaluation Procedure

From the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the 25010 — Systems and software quality requirements and evaluation (SQuaRE) will serve as the foundation for the evaluation tool that will be used to evaluate the

performance of the application. It includes the evaluation of quality management, acquisition, and maintenance.

The following procedure will be conducted to assess the performance of the Offline Signature System:

1. Train the Siamese Neural Network on the training set, using the appropriate training algorithm.
2. Use the test set to evaluate the performance of the trained Siamese Neural Network. This can be done by comparing the predicted similarity scores from the network with the true labels of the test set.
3. Measure the performance of the system using metrics such as accuracy, precision, recall, and F1-score.
4. Fine-tune the system to improve performance. This can be done by adjusting the parameters of the Siamese Neural Network, or by using different pre-processing or post-processing methods.
5. Randomly select thirty (30) signers to use the signature verification.
6. The web application will be evaluated by the respondents using the provided evaluation sheets and a 3-point Likert scale, as stated in Table 3.

7. Once the evaluation sheets have been processed, the data will be tallied to obtain the mean ratings.

SYSTEM EVALUATION (30%)	Weight	*Score*
A. FUNCTIONALITY		
1.1 Functions are required for the systems are implemented	3	
1.2 The system input and output are accurate	3	
1.3 The system modules are working and connected properly	3	
1.4 There is substantial system security	3	
B. PERFORMANCE/ USABILITY/ EFFICIENCY		
2.1 The system is error free (syntax, logic, run-time error)	3	
2.2 Easy to operate and remember	3	
2.3 Allows effective use of system resources	3	
C. MAINTAINABILITY / PORTABILITY/ DESIGN		
3.1 The system is easy to expand and modify to adapt to new changes	3	
3.2 The system can run on different environment	3	
3.3 The system Graphical user Interface design used was clear, neat and visible enough to be seen by the user.	3	
	Total	

Table 2. *Evaluation Form*

Scale	Descriptive Rating	Range
3	Highly Acceptable	2.5 - 2. 99
2	Acceptable	1.5 - 1.99
1	Not Acceptable	1.0 - 1.49

Table 3. *3- point Likert's Scale*

Work Plan

Table 4.

Work Breakdown Structure

Task	Objectives	Timeline	Expected Output
1. Literature Review	Review available literature on the signature verification and Siamese Neural Network model	1 month	Compilation of relevant research papers and understanding of the needs of the system to be developed
2. Data Collection	Collect the signature data for model training and testing	2 weeks	Clean and annotated signature data
3. Model Design	Design and train the model for signature verification using Siamese Neural Network	1 month	Trained Siamese Neural Network model
4. Model Evaluation	Evaluate the performance of the Siamese Neural Network model	1 month	Model evaluation report

5. UI Development	Develop a user interface for the system	1 month	User interface for a signature verification system
6. System Evaluation	Evaluate the performance of the offline signature verification system	1 month	System evaluation report
7. System Deployment	Deploy the signature verification system in a secure environment	2 weeks	Deployed and operational offline signature verification system using the Siamese Neural Network model

Chapter IV

RESULTS AND DISCUSSION

This chapter discusses the project description, project structure, project capabilities and limitations, and project evaluation.

PROJECT DESCRIPTION

Offline signature verification is a challenging problem in computer vision. The goal is to determine whether a given signature is genuine or forged. This is difficult because signatures can vary significantly from one signing to the next, even for the same person.

The project develops a signature verification system using a Siamese Neural Network, a type of deep learning architecture known for its effectiveness in learning similarity metrics. Siamese neural networks are a type of neural network that is well-suited for this task. It consists of two identical networks that are trained to learn the similarity between pairs of signatures. During training, the networks are presented with pairs of genuine and forged signatures. The primary goal of this project is to build a robust and accurate offline signature verification system using a Siamese Neural Network.

The project will involve the following steps:

1. Dataset Gathering: Collect a dataset of offline genuine and forged signatures images.
2. Data Processing: To ensure consistency and the best input for the Siamese Neural Network, do the necessary preprocessing operations on the acquired dataset, such as image normalization, noise removal, and resizing.
3. Siamese Neural Network Architecture: Designing and implementation of a Siamese neural network architecture suitable for signature verification.

4. Training: Utilize the prepared dataset to train the Siamese neural network. Implement suitable loss functions, such as contrastive loss to improve the model's ability to distinguish genuine signatures from forgeries.
5. Evaluation: Evaluate the performance of the Siamese neural network on a held-out test set.

PROJECT STRUCTURE

The project structure includes screenshot used in the program with its description and functions in the software.

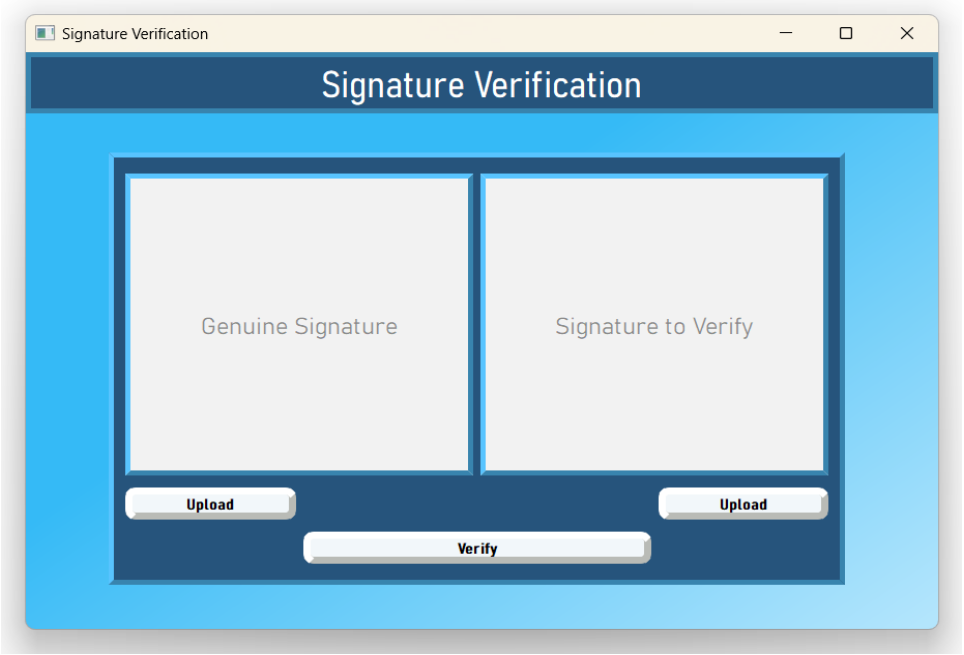

Figure 5. Offline Signature Verification User Interface

Figure 5 displays the user interface of the application; this includes the buttons for uploading and verifying signatures and a preview to display the uploaded signatures.

PROJECT CAPABILITIES AND LIMITATIONS

The following are the capabilities of the developed system:

1. The system effectively verifies offline signatures by comparing pairs of signature images and determining their similarity by reading the learned features such as pattern, stroke, and curvature of the signatures.
2. This signature verification applies the algorithm and technique of Siamese Neural Networks such as feature extraction and handling imbalance data on classifying genuine and forged signatures.
3. It saves time in obtaining samples because it performs one-shot learning which means it can make accurate predictions by a single sample in each class.
4. It focuses on verifying and capturing important variations on characteristics such as writing style, scaling, and thickness.
5. The system has a user-friendly interface that allows users to simply interact with the system and verify signatures by uploading signature images.

Just like any other system, this system has the following limitations:

1. The quality of the signature images, such as low resolution, noise, or distortions, may have an impact on the system's performance. Low-quality signature images could produce inaccurate or misleading findings.
2. It depends on the resolution of the static image and scan of the signature but not the dynamic qualities of the signature such as pressure on its application.
3. The system does not address online or real-time signature verification scenarios.
4. There is a struggle to determine and verify a fake signature with complexity or a signature with a very high resemblance to the real signature.

PROJECT EVALUATION

The system was evaluated by 30 evaluators. Evaluators consist of 15 non-technical and 15 technical.

TEST RESULTS

Table 5.

Functionality Test Result

System Module	Steps Undertaken	Results
Signature Upload Module	1. Clicked “Add Image” Button for the first signature 2. Clicked “Add Image” Button for the second signature 3, Clicked Submit button	1. System displayed the "Upload" button on the user interface, indicating the action to upload signature images for verification. 2. Offer options to remove individual or all uploaded signature images from the interface if the user wishes to start over or remove any incorrect or unwanted files. 3. System provides a confirmation message once the signature images have been successfully uploaded.

EVALUATION RESULTS

Table 6. *Evaluation Responses from 15 non-technical respondents*

A. Functionality				*B. Performance/Usability/Efficiency*			*C. Maintainability/Portability/Design*			*Total*
2	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*1*	*2*	*19*
3	*3*	*3*	*1*	*3*	*3*	*3*	*2*	*1*	*3*	*26*
2	*3*	*3*	*2*	*3*	*2*	*3*	*2*	*2*	*2*	*24*
2	*3*	*2*	*2*	*3*	*1*	*1*	*3*	*2*	*1*	*20*
2	*3*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*21*
1	*2*	*2*	*2*	*1*	*1*	*2*	*2*	*2*	*2*	*17*
2	*2*	*3*	*1*	*1*	*3*	*3*	*2*	*3*	*3*	*26*
2	*2*	*2*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*24*
2	*1*	*1*	*1*	*1*	*2*	*2*	*2*	*2*	*2*	*16*
2	*1*	*2*	*1*	*1*	*2*	*1*	*2*	*2*	*1*	*15*
2	*2*	*1*	*3*	*2*	*2*	*2*	*2*	*2*	*1*	*19*
2	*2*	*2*	*3*	*2*	*2*	*2*	*2*	*3*	*2*	*22*
3	*2*	*3*	*2*	*3*	*2*	*3*	*2*	*2*	*3*	*25*
2	*3*	*3*	*2*	*2*	*2*	*3*	*2*	*1*	*2*	*22*
3	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*2*	*3*	*28*

Table 7. *Evaluation Responses from 15 technical respondents*

A. Functionality				*B. Performance/Usability/Efficiency*			*C. Maintainability/Portability/Design*			*Total*
3	*2*	*3*	*2*	*3*	*2*	*3*	*2*	*2*	*3*	*25*
3	*3*	*3*	*1*	*3*	*3*	*3*	*2*	*1*	*3*	*26*
2	*3*	*3*	*2*	*3*	*2*	*3*	*2*	*2*	*2*	*24*
3	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*2*	*3*	*28*
2	*3*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*21*
3	*2*	*3*	*2*	*3*	*2*	*3*	*2*	*2*	*3*	*25*
2	*2*	*3*	*1*	*1*	*3*	*3*	*2*	*3*	*3*	*26*
2	*2*	*2*	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*24*
2	*3*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*21*
2	*3*	*2*	*2*	*2*	*2*	*2*	*2*	*2*	*1*	*20*
2	*2*	*1*	*3*	*2*	*2*	*2*	*2*	*2*	*1*	*19*
2	*2*	*2*	*3*	*2*	*2*	*2*	*2*	*3*	*2*	*22*
3	*2*	*3*	*2*	*3*	*2*	*3*	*2*	*2*	*3*	*25*
2	*3*	*3*	*2*	*2*	*2*	*3*	*2*	*1*	*2*	*22*
3	*3*	*3*	*3*	*3*	*3*	*3*	*3*	*2*	*3*	*28*

The evaluation results from 30 respondents are equal to 22.67 or 23 total mean points. Dividing the respondents between technical and non-technical, the non-technical respondents have a total mean score of 21.6 or 22. Meanwhile, the technical respondents have a 23.73 or 24 total mean score.

CHAPTER V

SUMMARY OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

This chapter contains the summary of findings, conclusions, and recommendations derived to further improve the system.

Summary of Findings

In this study, Siamese Neural Network was utilized to implement an offline signature verification system. The dataset comprised signatures from 22 individuals, with each person contributing 24 genuine signatures and 30 forged signatures. The objective was to develop a system capable of distinguishing genuine and forged signatures.

The Siamese neural network was trained on the provided dataset, which consisted of paired signatures for comparison. The network learned to extract relevant features and measure the similarity between two signatures. During the training process, the network was optimized to minimize the distance between genuine signatures and maximize the distance between genuine and forged signatures.

After training the Siamese neural network, it was evaluated on a separate test dataset to assess its performance. The results indicated that the system was successful in detecting whether a given signature was genuine or forged. The accuracy of the system in making these distinctions was high, demonstrating its effectiveness in offline signature verification.

However, it's important to consider the system constraints associated with offline signature verification. These constraints include the process of capturing and uploading the signatures, as well as the physical environment in which the signatures were made. Factors such as the quality of the signature capture device, the lighting conditions, and the writing utensils used (e.g., pen type) can potentially impact the accuracy of the system.

Conclusion

The study's findings highlight the viability of using a Siamese neural network for offline signature verification. By leveraging the power of deep learning, the system was able to learn discriminative features and effectively differentiate between genuine and forged signatures.

The success of the Siamese neural network suggests that it can be a valuable tool in various applications, such as fraud detection and document authentication. Its ability to accurately identify forged signatures has significant implications in fields where signature verification plays a crucial role, such as banking, legal documentation, and personal identification.

However, it's important to acknowledge the impact of system constraints on the performance of the system. The process of capturing and uploading signatures, as well as the physical environment in which the signatures were made, can introduce variations that may affect the system's accuracy. Therefore, it is necessary to ensure standardized procedures for signature capture and consider the limitations of the physical environment when deploying the system in practical settings.

Overall, the project demonstrates the potential of Siamese neural networks for offline signature verification and provides a solid foundation for future advancements in this field. Future research can focus on addressing the challenges posed by output/system constraints to improve the system's robustness and real-world applicability.

Recommendation

The following recommendations are provided for future work in the field of signature verification using Siamese Neural Networks:

1. Utilize a larger and more diverse dataset that encompasses a wide range of signatures from different demographics and writing styles. Instead of relying solely on open-source websites

like Kaggle, consider collecting a dataset specifically tailored to the requirements of the research.

2. Explore collaborations with industry partners or institutions such as banks, legal institutions, or government agencies. Such collaborations can provide access to unique and proprietary datasets containing genuine and forged signatures collected from authentic sources.
3. Deploy the model in a more user-friendly interface. To enhance the usability and practicality of the signature verification system, consider developing a user-friendly interface that allows users to directly sign on to the system instead of uploading pre-captured images. This real-time signature input capability would enable a more seamless and intuitive user experience.

REFERENCES

[1] Shrestha, N., Ghimire, P. S., Neupane, S., & Pokharel, S. (2017, August). *Offline Signature Verification Using Convolutional Neural Network.* https://www.researchgate.net/publication/337084834_Offline_Signature_Verification_Using_Convolutional_Neural_Network_Undergraduate_Project_Subject_Code_CT_707

[2] Dey, S., Dutta, A., Toledo, J. I., Ghosh, S. K., & Llad´os, J. (2017, July). *SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification*. https://www.researchgate.net/publication/318316051_SigNet_Convolutional_Siamese_Network_ for_Writer_Independent_Offline_Signature_Verification

[3] Ebrahim, A., Kolivand, H., Rehman, A., Rahim, M., & Saba, T. (2018). *Features selection for offline handwritten signature verification: Current state of the art* [Review of *Features selection for offline handwritten signature verification: Current state of the art*]. LJMU Research Online.http://researchonline.ljmu.ac.uk/id/eprint/9857/3/Features%20selection%20for%20offline%20handwritten%20signature%20verification.pdf

[4] Chakraborty, S. (2019). Siamese Triple Ranking Convolution Network in Signature Forgery Detection.

Www.academia.edu.

https://www.academia.edu/86862386/Siamese_Triple_Ranking_Convolution_Network_in_Signature_Forgery_Detection

[5] Sharma, N., Gupta, S., & Mehta, P. (2021). A Comprehensive Study on Offline Signature Verification. *Journal of Physics: Conference Series*, *1969*(1), 012044. https://doi.org/10.1088/1742-6596/1969/1/012044

[6] B. Akhila, G. Nikhila, A. Lakshmi, G. Jahnavi, & Mrs. J. Himabindhu. (2021). *Signature Verification Using Image Processing And Neural Networks*. International Journal Of Creative Research Thoughts (IJCRT). https://ijcrt.org/papers/IJCRT2108073.pdf

[7] Rahman, M., Miraz Mahfuz, S., & Al-Mamun, S. (2019). Writer-independent Offline Handwritten Signature Verification using Novel Feature Extraction Techniques. *International*

Journal of Computer Applications, *177*(14), 975–8887. https://www.ijcaonline.org/archives/volume177/number14/rahman-2019-ijca-919537.pdf

[8] Al-banhawy, N. H., Al-Azhar University, E., Mohsen, H., Ghali, N., Egypt, F. U. in, & Egypt, F. U. in. (2020). Signature Identification And Verification Systems: A Comparative Study On The Online And Offline Techniques. *Future Computing and Informatics Journal*, *5*(1), 28. https://www.academia.edu/91219590/Signature_Identification_and_Verification_Systems_A_Comparative_Study_on_the_Online_and_Offline_Techniques

[9] Aufar, Y., & Sitanggang, I. S. (2022). Face recognition based on Siamese convolutional neural network using Kivy framework. *Indonesian Journal of Electrical Engineering and Computer Science*, *26*(2), 764. https://www.academia.edu/89297336/Face_recognition_based_on_Siamese_convolutional_neural_network_using_Kivy_framework

[10] Pulabaigari, V. (2019). OSVNet: Convolutional Siamese Network for Writer Independent Online Signature Verification. *2019 International Conference on Document Analysis and Recognition (ICDAR)*. https://www.academia.edu/72522027/OSVNet_Convolutional_Siamese_Network_for_Writer_Independent_Online_Signature_Verification

[11] Wiggers, K. L., Britto, A. S., Heutte, L., Koerich, A. L., & Oliveira, L. S. (2019). Image Retrieval and Pattern Spotting using Siamese Neural Network. *2019 International Joint Conference on Neural Networks (IJCNN)*. https://www.academia.edu/62287523/Image_Retrieval_and_Pattern_Spotting_using_Siamese_Neural_Network

[12] Kumari, K., & Rana, S. (2018). Offline Signature Verification using Intelligent Algorithm. *International Journal of Engineering & Technology*, *7*(4.12), 69. https://www.academia.edu/53195687/Offline_Signature_Verification_using_Intelligent_Algorithm

[13] Abdalhaleem, A., Barakat, B. K., & El-Sana, J. (2018). *Case Study: Fine Writing Style Classification Using Siamese Neural Network.* IEEE Xplore. https://doi.org/10.1109/ASAR.2018.8480212

[14] Shaikh, W., Nishad, R., Rai, S., & Shaikh, S. (2021). *Ar Based Signature Verification*. International Research Journal of Engineering and Technology (IRJET). https://www.irjet.net/archives/V8/i5/IRJET-V8I5232.pdf

[15] Kanawade, M., & Katariya, S. (n.d.). *OFFLINE SIGNATURE VERIFICATION AND RECOGNITION*. Retrieved from http://www.tjprc.org/publishpapers/2-16-1374732222-13.Offline%20signature.full.pdf

[16] M. Muzaffar Hameed, Ahmad, R., Laiha, M., & Murtaza, G. (2021, January 13). Machine learning-based offline signature verification systems: A systematic review. Retrieved January 27, 2023, from ResearchGate website: https://www.researchgate.net/publication/348475222_Machine_learning-based_offline_signature_verification_systems_A_systematic_review

[17] Jagtap, A. (2020, December). *Verification of genuine and forged offline signatures using Siamese Neural Network (SNN)*. ResearchGate. Retrieved January 26, 2023, from https://www.researchgate.net/publication/340388072_Verification_of_genuine_and_forged_offl i ne_signatures_using_Siamese_Neural_Network_SNN