Journal of Software Engineering and Applications, 2024, 17, 214-227
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

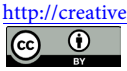
Dynamic Signature Verification Using Pattern Recognition

Emmanuel Nwabueze Ekwonwune[1], Duroha Austin Ekekwe[2], Chinyere Iheakachi Ubochi[1], Henry Chinedu Oleribe[3]

[1]Department of Computer Science, Imo State University, Owerri, Nigeria
[2]Department of Computer Science, Gregory University, Abia, Nigeria
[3]ICT Department, Alvan Ikoku University of Education, Owerri, Nigeria
Email: Ekwonwuneemmanuel@Yahoo.com

How to cite this paper: Ekwonwune, E.N., Ekekwe, D.A., Ubochi, C.I. and Oleribe, H.C. (2024) Dynamic Signature Verification Using Pattern Recognition. *Journal of Software Engineering and Applications*, **17**, 214-227.
https://doi.org/10.4236/jsea.2024.175012

Received: April 13, 2024
Accepted: May 24, 2024
Published: May 27, 2024



Abstract

Dynamic signature is a biometric modality that recognizes an individual's anatomic and behavioural characteristics when signing their name. The rampant case of signature falsification (Identity Theft) was the key motivating factor for embarking on this study. This study was necessitated by the damages and dangers posed by signature forgery coupled with the intractable nature of the problem. The aim and objectives of this study is to design a proactive and responsive system that could compare two signature samples and detect the correct signature against the forged one. Dynamic Signature verification is an important biometric technique that aims to detect whether a given signature is genuine or forged. In this research work, Convolutional Neural Networks (CNNsor ConvNet) which is a class of deep, feed forward artificial neural networks that has successfully been applied to analysing visual imagery was used to train the model. The signature images are stored in a file directory structure which the Keras Python library can work with. Then the CNN was implemented in python using the Keras with the TensorFlow backend to learn the patterns associated with the signature. The result showed that for the same CNNs-based network experimental result of average accuracy, the larger the training dataset, the higher the test accuracy. However, when the training dataset are insufficient, better results can be obtained. The paper concluded that by training datasets using CNNs network, 98% accuracy in the result was recorded, in the experimental part, the model achieved a high degree of accuracy in the classification of the biometric parameters used.

Keywords

Verification, Security, Biometrics, Signature, Authentication, Model,

Pattern Recognition, Dynamic

1. Introduction

Signature verification is an important biometric technique that aims to detect whether a given signature is genuine or forged. It is important in preventing falsification of documents in numerous financial, legal, and other commercial organisation. There are two main kinds of signature verification: static and dynamic. Static, or offline verification is the process of verifying a document signature after it has been made, while dynamic or online verification takes place as a person creates his/her signature on a digital tablet or a similar device. The signature in question is then compared to previous samples of that person's signature set up in the database. This is a comparative analysis of different already known deep learning architectures to check which of those performs the best on the classification. It was solely for offline handwritten signatures.

A model that can learn from signatures and make predictions as to whether the signature in question is forged or otherwise has been successfully implemented. This model can be deployed at various government offices where handwritten signatures are used as a means of approval or authentication. While this method uses CNNs to learn the signatures, the structure of our fully connected layer is not optimal. This implementation may be considered extreme. In the model created in this work, two classes are created for each user (Real and forgery). "Convolutional neural networks are variants of multilayer perception, designed to emulate the behaviour of a visual cortex" [1]. These models mitigate the challenges posed by the MLP architecture by exploiting the strong spatially local correlation present in natural images. As opposed to MLPs, CNNs have the following distinguishing features: 3D, local connectivity, shared weight, and pooling. The convolutional layer is the core building block of a CNN.

1.1. Background of the Study

The problems associated with signature forgery are enormous and cannot be overemphasised. Forged signature can result to poor judgement, wrong choice, economic loss, deceit etc. by an individual, private organisation or even government agencies. A lot of persons have been enjoying unmerited favours, business and employment opportunities, and juicy appointed positions etc using documents with forged signatures. This menace is more prevalent in our clime where more emphasis are placed on paper qualifications.

Over time, different options of signature verification have been in use, unfortunately, the problems and incidences of forgery have proved to be intractable. This is where Dynamic Signature Verification using Pattern Recognition rightly comes in. It combines the physical signature signing and other biometric parameters in its functionalities.

1.2. Statement of the Problem

This research work was embarked upon in order to deal with problems associated with forged signatures (identity theft), such problems include deceit, poor judgement, wrong choices, economic loss etc.

1.3. Aim and Objectives of the Study

The aim of the proposed system is to recognize any alpha-numeric characters used by any individual as a signature. The alpha numerals are represented as patterns.

The objectives of the study include the following

1) To design a computer technology that is capable of training a data model that can compare any two sample signatures for a match.

2) To use the same computer technology to identify the real signature and the forged one between two sample signatures.

2. Review of Related Literature

The execution of a signature depends on a very complex system, strongly influenced by behavioural and social conditions. As a result, two repetitions of a signature from the same writer never have an identical appearance. This effect is known as intrapersonal variability. Consequently, many systems have different effective error rates for verifying the authenticity of a signature, depending on the training conditions.

More specifically, two of the challenges faced in signature verification are intra-class variability where the individual has slight variations in their own signature writing styles over a period of time, and inter-class variability where some other person tries to mimic or simulate the signature of an individual to get an illicit access through a signature verification system.

Signature verification techniques utilize many different characteristics of an individual's signature in order to authenticate that individual. The advantages of using such an authentication technique are; 1) signatures are widely accepted by society as a form of verification C 2) information required is not sensitive and 3) forging of an individual's signature does not mean a long-life loss of that individual's identity. The general idea here is to determine the signature verification technique which is not costly to build, user friendly in terms of configuration, robust against imposters and is reliable even if the individual is under different emotions [2].

An innovative approach utilizing a time-aligned recurrent neural network (TA-RNN) for the task of verifying signatures online. This method employs deep learning techniques to extract signature features from a database. It leverages an RNN to process the training data necessary for verifying signatures, which helps decrease the time needed for identification. The TA-RNN method, when compared to alternative methods, enhances the accuracy and speed of the signature verification process. Nonetheless, the verification process within this

system requires a considerable amount of time to complete [3].

An adaptable fingerprint authentication system incorporating linear convolution for biometric applications was suggested. The system utilizes linear convolutional functions and vectors to furnish pertinent information for authentication purposes. Feature extraction techniques are applied to isolate essential patterns and features within signatures. This proposed system aims to optimize accuracy and efficiency in both verification and recognition, ultimately bolstering security throughout the authentication process [4].

The presentation of a model for offline signature verification, combining convolutional neural network (CNN) and capsule neural network (CapsNet) architectures. The CNN focuses on identifying key features, patterns, and factors within signatures, contributing essential data to the signature verification model. CapsNet is employed to streamline computational complexity. Experimental outcomes demonstrated that the proposed model enhances accuracy in signature verification, thereby elevating the overall performance of biometric systems [5].

The HELR classifier is employed to identify features and patterns inherent in biometric signatures, predicting precise information crucial for the verification process. By leveraging HELR, the security of signatures is heightened, resulting in elevated accuracy in verification and improved feasibility and effectiveness of biometric systems. It is worth noting that the proposed protocol demands increased computational effort during the deviation of biometric patterns [6].

A single template matching approach using local stability-weighted dynamic time warping (LS-DTW) for online signature verification. LS-DTW is employed to derive optimal warping templates, reducing computational complexity. These templates, trained and generated for the matching method, effectively identify user signatures. In comparison to alternative methods, the proposed approach attains high verification accuracy, enhancing system performance and mobility [7].

Machine Learning algorithms are employed to boost verification effectiveness, with Deep BiLSTM utilized for extracting static and dynamic features from signatures. The score-level fusion emphasizes obtaining optimal information for verification, enhancing efficiency and reliability in online signature verification. However, challenges arise in managing complex patterns with the score-level fusion approach [8].

Online signature verification technique incorporating down sampling and signer-dependent sampling frequency. The sampling frequency range is determined by specific vectors and functions, offering pertinent information for signature verification and decreasing computation time. Experimental outcomes indicate the method's success in achieving high accuracy in both verification and prediction, thereby enhancing the efficiency of biometric systems [9].

Presented an offline signature verification model utilizing graph neural networks (GNN). Target nodes in the graphs are identified through features essential for prediction, detection, and recognition processes. Training of test signa-

ture samples is focused on these target nodes, reducing latency in the identification process. The introduced GNN-based model enhances verification accuracy, ensuring effective services for users [10].

"*Pattern Recognition* is a mature but exciting and fast developing field, which underpins developments in cognate fields such as computer vision, image processing, text and document analysis and neural networks. It is closely akin to machine learning, and also finds applications in fast emerging areas such as biometrics, bioinformatics, multimedia data analysis and most recently data science" [11].

The theory that supports pattern recognition system is the Template Matching Theory The theory describes the most basic approach to Human Pattern Recognition. The theory assumes that every perceived object is stored as a template into long term memory. Incoming information is compared with these to find an exact match.

2.1. Pattern Recognition System

A pattern recognition system is a computational framework designed to identify and interpret patterns within data. It encompasses various techniques and algorithms to analyse and classify patterns in fields such as image processing, speech recognition and data mining [12].

2.2. Structure of a Pattern Recognition System

A pattern recognition system, regardless of the specific method employed, typically comprises three interconnected and distinct processes. The first involves data construction, where original information is transformed into a vector format suitable for computer processing. The subsequent processes are pattern analysis and pattern classification. Pattern analysis is responsible for manipulating the data vector through tasks like feature selection, feature extraction, and data-dimension compression.

The primary objective of pattern classification is to harness the insights gained from pattern analysis, guiding the computer to execute classification tasks effectively. The pattern recognition system commonly follows a five-step approach, with the classification/regression/description step, as depicted in **Figure 1**, serving as the core of the system. Classification, a key problem in pattern recognition, entails assigning an object to a specific class. The system's output is typically an integer label, such as categorizing a product as "1" or "0" in a quality control scenario. Regression serves as an extension of a classification task within the pattern recognition system, where the system's output is a numerical value. For instance, it involves predicting the stock value of a company by considering factors like its historical performance and stock market indicators. Description, on the other hand, involves representing an object through a series of primitives, and the pattern recognition system generates a structural or linguistic description accordingly.

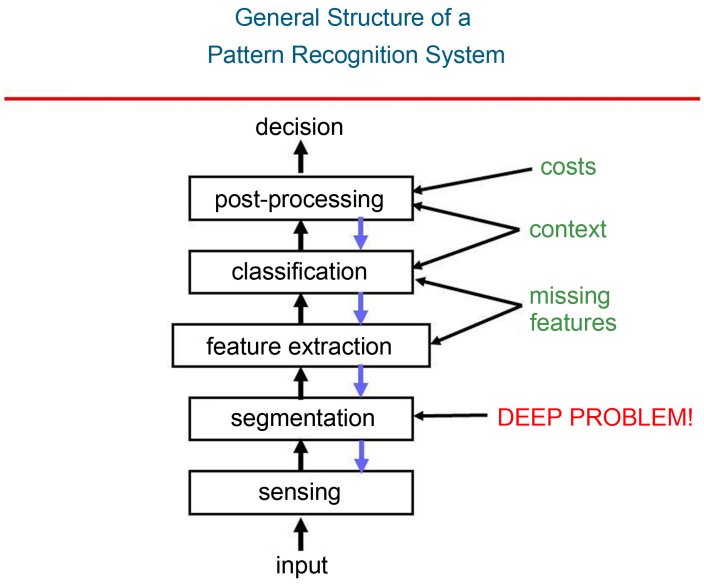


Figure 1. Composition of a PR system.

2.3. The Classification of Pattern Recognition System

1) Rule based system;
2) Classical fuzzy;
3) System Bayesian system;
4) Neural networks system;
5) Fuzzy neural networks systems.

2.4. Methods of Pattern Recognition

1) Statistical pattern recognition

This pattern recognition approach uses historical statistical data that learns from patterns and examples. The method collects observations and processes them to define a model. This model then generalizes over the collected observations and applies the rules to new datasets or examples [13].

2) Syntactic pattern recognition

Syntactic pattern recognition involves complex patterns that can be identified using a hierarchical approach. Patterns are established based on the way primitives (e.g., letters in a word) interact with each other. An example of this could be how primitives are assembled in words and sentences. Such training samples will enable the development of grammatical rules that demonstrate how sentences will be read in the future [13].

3) Neural pattern recognition

This method uses artificial neural networks (ANN) and learns from complex and non-linear input/output relations, adapts to data, and detects patterns. The most popular and effective method in neural networks is the feed-forward method. In this method, learning happens by giving feedback to input patterns. This is much like humans learning from their past experiences and mistakes.

The ANN-based model is rated as the most expensive pattern recognition method compared to other methods due to the computing resources involved in the process [13].

4) Template matching

Template matching is one of the simplest of all pattern recognition approaches. Here, the similarity between two entities is determined by matching the sample with the reference template. Such methods are typically used in digital image processing, where small sections of an image are matched to a stored template image. Some of its real-world examples include medical image processing, face recognition, and robot navigation [13].

5) Fuzzy-based approach

In the fuzzy approach, a set of patterns are partitioned based on the similarity in the features of the patterns. When the unique features of a pattern are correctly detected, data can be easily classified into that known feature space. Even the human visual system sometimes fails to recognize certain components despite scanning objects for a long time. The same holds true for the digital world, where algorithms cannot figure out the exact nature of an object. Hence, the fuzzy approach aims to classify objects based on several similar features in the detected patterns [13].

6) Hybrid approach

A hybrid approach employs a combination of the above methods to take advantage of all these methods. It employs multiple classifiers to detect patterns where each classifier is trained on a specific feature space. A conclusion is drawn based on the results accumulated from all the classifiers [13].

Pattern Recognition Applications (**Figure 2**)

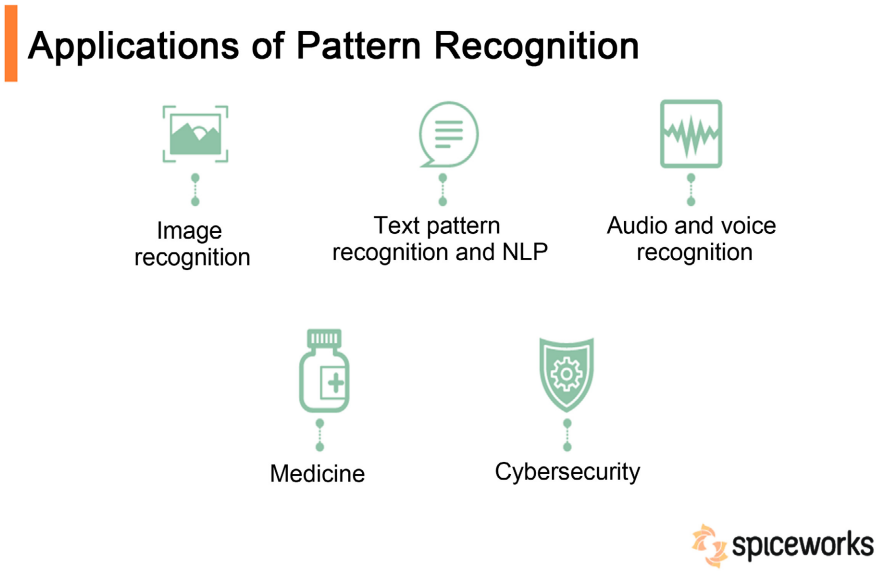


Figure 2. Application of pattern recognition system. Source: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-pattern-recognition/ [13].

3. Methodology and Analysis

[14] Signature recognition is an example of behavioural biometrics that identifies a person based on their handwriting. It can be operated in two different ways.

Static: In this mode, users write their signature on paper, and after the writing is complete, it is digitized through an optical scanner or a camera to turn the signature image into bits [14]. The biometric system then recognizes the signature analysing its shape. This group is also known as "off-line" [15].

Dynamic: In this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDAs. Some systems also operate on smart-phones or tablets with a capacitive screen, where users can sign using a finger or an appropriate pen. Dynamic recognition is also known as "on-line". Dynamic information usually consists of the following information: [15]

1). spatial coordinate x(t) 2). spatial coordinate y(t) 3). pressure p(t)

4). azimuth az(t) 5). inclination in(t) 6). pen up/down

From Wikipedia, the free encyclopedia (See **Figure 3** and **Figure 4** below):

1) Example of signature shape.

2) Example of dynamic information of a signature. Looking at the pressure information it can be seen that the user has lifted the pen 3 times in the middle of the signature (areas with pressure equal to zero) (Source: Wikipedia).

The Proposed System

The figure below shows the High-Level model (HLM) for the proposed system.

The figure below shows the architectural framework for a dynamic signature verification using pattern recognition (**Figure 5** below).

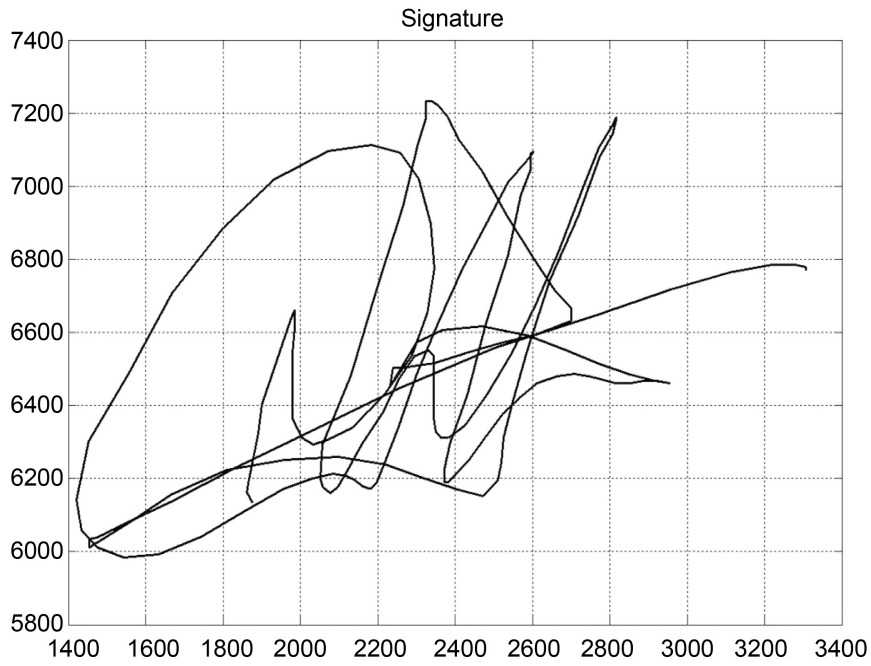


Figure 3. Pattern Recognition Source: Wikipedia, The free Encyclopedia.

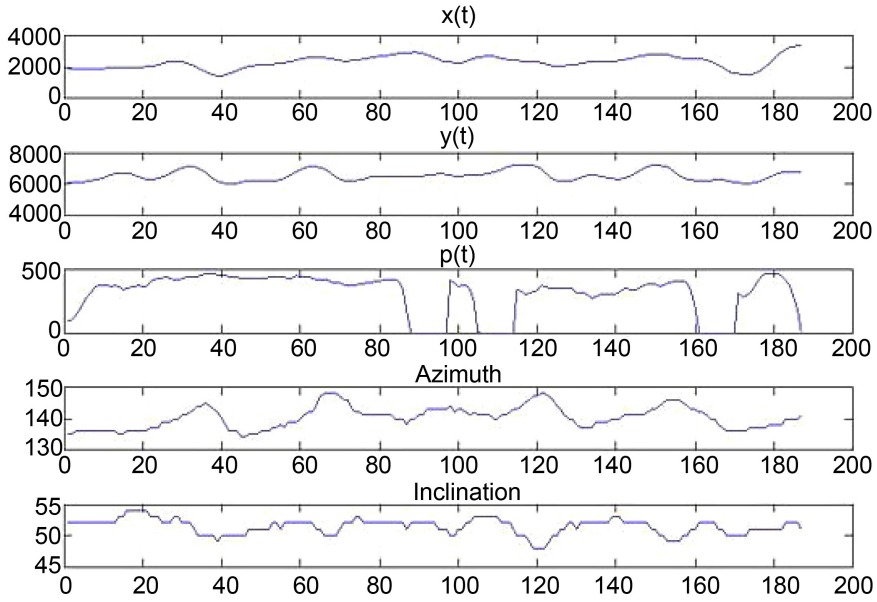


Figure 4. Pattern Recognition Source: Wikipedia, the Free Encyclopedia.

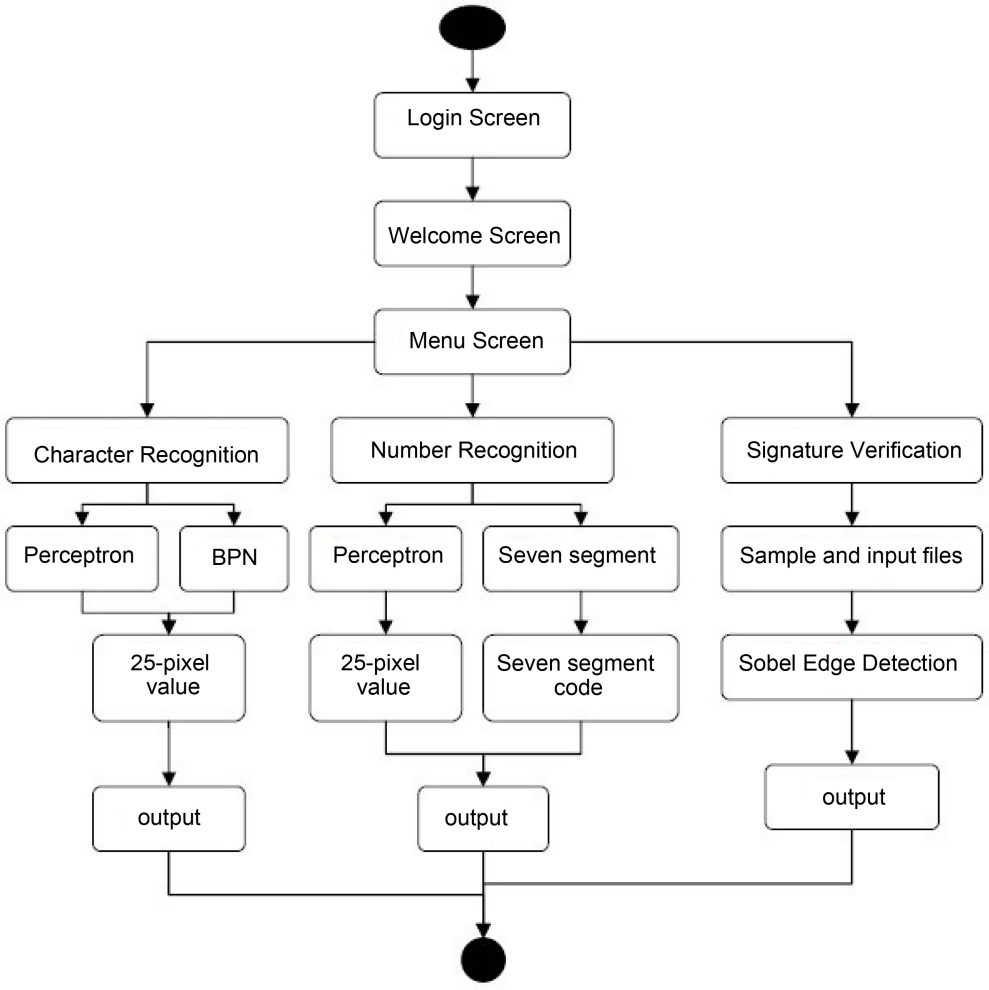


Figure 5. The high level model of dynamic signature verification using pattern recognition.

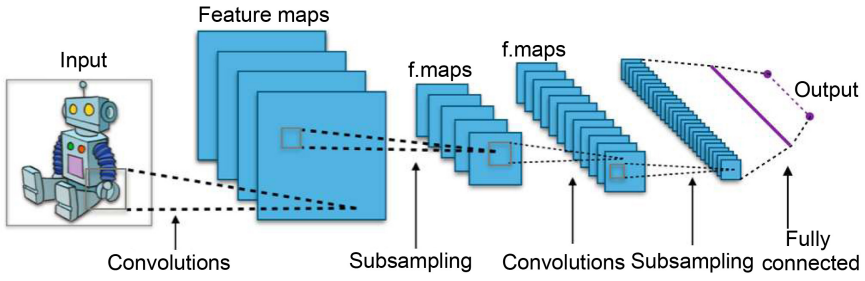


Figure 6. The architecture of signature verification system. Source: Chapran. J. (2006) [16].

In the signature recognition biometric process, variables such as the acceleration, wave, speed and velocity are as important as the signature's dynamic/static shape. Neural network tech can also be integrated into these components, enabling the biometric to identify even the slightest of variations in the approach taken by a signee. With neural networks, the database that houses the verification and enrolment templates can also be updated in real time.

In terms of practical use, the process of signature recognition involves the use of a specialized writing device and a pen, which is connected to a centralized server for data processing. For data capture during enrolment, the person has to compose his/her signature multiple times on the device. Unfortunately, there's more than one constraint to this data acquisition phase (See **Figure 6** above).

First, the signature needs to be of a specific length. It shouldn't be too short or too long. For example, in the case of a long signature, a large quantity of behavioural data will be captured. Hence, it can be challenging for a signature recognition device to classify any unique or consistent data points. In terms of short signatures, not enough behavioural data will be collected, thus resulting in a higher FAR (False Acceptance Rate).

Dynamic signature recognition uses multiple characteristics in the analysis of an individual's handwriting. These characteristics vary in use and importance from vendor to vendor and are collected using contact sensitive technologies, such as PDAs or digitizing tablets, which acquires the signature in real time.

Most of the features used are dynamic characteristics rather than static and geometric characteristics, although some vendors also include these characteristics in their analyses. Common dynamic characteristics include the velocity, acceleration, timing, pressure, and direction of the signature strokes, all analyzed in the X, Y, and Z directions.

The X and Y position are used to show the changes in velocity in the respective directions while the Z direction is used to indicate changes in pressure with respect to time.

Some dynamic signature recognition algorithms incorporate a learning function to account for the natural changes or drifts that occur in an individual's signature over time. The most popular pattern recognition techniques applied for signature recognition are dynamic time warping, hidden Markov models and

vector quantization. Combinations of different techniques also exist.

The characteristics used for dynamic signature recognition are almost impossible to replicate. Unlike a graphical image of the signature, which can be replicated by a trained human forger, a computer manipulation, or a photocopy, dynamic characteristics are complex and unique to the handwriting style of the individual. Despite this major strength of dynamic signature recognition, the characteristics historically have a large intra-class variability (meaning that an individual's own signature may vary from collection to collection), often making dynamic signature recognition difficult. Recent research has reported that static writing samples can be successfully analysed to overcome this issue.

Convolutional Neural Networks (CNNs or ConvNet) which is a class of deep, feed forward artificial neural networks that has successfully been applied to analysing visual imagery was used to train the model. Convolutional Neural Network is a regularized type of feed-forward neural network that learns feature engineering by itself via filters (or kernel) optimization. Vanishing gradients and exploding gradients, seen during backpropagation in earlier neural networks, are prevented by using regularized weights over fewer connections. For example, for *each* neuron in the fully-connected layer, 10,000 weights would be required for processing an image sized 100 × 100 pixels. However, applying cascaded *convolution* (or cross-correlation) kernels only 25 neurons are required to process 5 × 5-sized tiles. Higher-layer features are extracted from wider context windows, compared to lower-layer features [17].

They have applications in:

- image and video recognition,
- recommender systems,
- image classification,
- image segmentation,
- medical image analysis,
- natural language processing,
- brain–computer interfaces, and
- financial time series.

4. Architecture

A convolutional neural network consists of an input layer, hidden layers and an output layer. In a convolutional neural network, the hidden layers include one or more layers that perform convolutions. Typically this includes a layer that performs a dot product of the convolution kernel with the layer's input matrix. This product is usually the Frobenius inner product, and its activation function is commonly ReLU. As the convolution kernel slides along the input matrix for the layer, the convolution operation generates a feature map, which in turn contributes to the input of the next layer. This is followed by other layers such as pooling layers, fully connected layers, and normalization layers. Here it should be noted how close a convolutional neural network is to a matched filter [17].

5. Image Recognition

CNNs are often used in image recognition systems. In 2012, an error rate of 0.23% on the MNIST database was reported. Another paper on using CNN for image classification reported that the learning process was "surprisingly fast"; in the same paper, the best published results as of 2011 were achieved in the MNIST database and the NORB database. Subsequently, a similar CNN called AlexNet won the ImageNet Large Scale Visual Recognition Challenge 2012.

When applied to facial recognition, CNNs achieved a large decrease in error rate. Another paper reported a 97.6% recognition rate on "5600 still images of more than 10 subjects". CNNs were used to assess video quality in an objective way after manual training; the resulting system had a very low root mean square error.

The ImageNet Large Scale Visual Recognition Challenge is a benchmark in object classification and detection, with millions of images and hundreds of object classes. In the ILSVRC 2014, a large-scale visual recognition challenge, almost every highly ranked team used CNN as their basic framework. The winner GoogLeNet (the foundation of DeepDream) increased the mean average precision of object detection to 0.439329, and reduced classification error to 0.06656, the best result to date. Its network applied more than 30 layers. That performance of convolutional neural networks on the ImageNet tests was close to that of humans. The best algorithms still struggle with objects that are small or thin, such as a small ant on a stem of a flower or a person holding a quill in their hand. They also have trouble with images that have been distorted with filters, an increasingly common phenomenon with modern digital cameras. By contrast, those kinds of images rarely trouble humans. Humans, however, tend to have trouble with other issues. For example, they are not good at classifying objects into fine-grained categories such as the particular breed of dog or species of bird, whereas convolutional neural networks handle this. A many-layered CNN demonstrated the ability to spot faces from a wide range of angles, including upside down, even when partially occluded, with competitive performance. The network was trained on a database of 200,000 images that included faces at various angles and orientations and a further 20 million images without faces. They used batches of 128 images over 50,000 iterations [17].

The signature images are stored in a file directory structure which the Keras Python library can work with. Then the CNN was implemented in python using the Keras with the TensorFlow backend to learn the patterns associated with the signature.

6. Conclusion and Recommendations

6.1. Conclusion

The paper concluded that by training datasets using CNNs network, 98% accuracy result was recorded, in the experimental part, the model achieved high degree of accuracy in the classification of the biometric parameters used.

6.2. Recommendation

Based on the conclusion above, it is recommended that:

1) Dynamic signature verification using pattern recognition is the best bet anywhere effective signature verification is desired.

2) Individuals, organisations, institutions and governments should as a matter of urgency adopt the dynamic signature verification using pattern recognition system.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Rawlson, K. (2016) Explainer: Signature Recognition. https://www.biometricupdate.com/201601/explainer-signature-recognition

[2] Vacca, S. (2007) Biometric Information System: Pattern Recognition Approach. *Journal of Business Research*, **2**, 78-84.

[3] Tolosana, R., Vera-Rodriguez, R., Fierrez, J. and Ortega-Garcia, J. (2021) DeepSign: Deep On-Line Signature Verification. *The IEEE Transactions on Biometrics, Behavior, and Identity Science*, **3**, 229-239. https://doi.org/10.1109/TBIOM.2021.3054533

[4] Yang, X., Zhu, H., Wang, F., Zhang, S., Lu, R. and Li, H. (2021) MASK: Efficient and Privacy-Preserving M-Tree Based Biometric Identification over Cloud. *Peer-to-Peer Networking and Applications*, **14**, 2171-2186. https://doi.org/10.1007/s12083-021-01120-7

[5] Parcham, E., Ilbeygi, M. and Amini, M. (2021) CBCapsNet: A Novel Writer-Independent Offline Signature Verification Model Using a CNN-Based Architecture and Capsule Neural Networks. *Expert Systems with Applications*, **185**, 115649. https://doi.org/10.1016/j.eswa.2021.115649

[6] Bassit, A., Hahn, F., Peeters, J., Kevenaar, T., Veldhuis, R. and Peter, A. (2021) Fast and Accurate Likelihood Ratio-Based Biometric Verification Secure against Malicious Adversaries. *IEEE Transactions on Information Forensics and Security*, **16**, 5045-5060. https://doi.org/10.1109/TIFS.2021.3122823

[7] Okawa, M. (2020) Online Signature Verification Using Single-Template Matching with Time-Series Averaging and Gradient Boosting. *Pattern Recognition*, **102**, 107227. https://doi.org/10.1016/j.patcog.2020.107227

[8] Dhieb, T., Boubaker, H., Njah, S., Ben Ayed, M. and Alimi, A.M. (2022) A Novel Biometric System for Signature Verification Based on Score Level Fusion Approach. *Multimedia Tools and Applications*, **81**, 7817-7845. https://doi.org/10.1007/s11042-022-12140-7

[9] Saleem, M. and Kovari, B. (2021) Online Signature Verification Using Signature Down-Sampling and Signer-Dependent Sampling Frequency. *Neural Computing. Applications*, 1-13.

[10] Roy, S., Sarkar, D., Malakar, S. and Sarkar, R. (2021) Offline Signature Verification System: A Graph Neural Network Based Approach. *Journal of Ambient Intelligence and Humanized Computing*, **14**, 1-11. https://doi.org/10.1007/s12652-021-03592-0

[11] (2019) Signature Verification System. Elsevier Journal Publishers. https://www.elsevier.marketing/journal/Pattern-Recognition

[12] Petrou, M. (2001) Learning in Pattern Recognition: Some Thoughts. *Pattern Recognition Letters*, **22**, 3-13. https://doi.org/10.1016/S0167-8655(00)00094-5

[13] https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-pattern-recognition/

[14] Ismail, M.A. and Gad, Samia (2000) Off-Line Arabic Signature Recognition and Verification. *Pattern Recognition*, **33**, 1727-1740. https://doi.org/10.1016/S0031-3203(99)00047-3

[15] (2016) Explainer: Signature Recognition. Biometric Update. https://en.m.wikipedia.org/wiki/Signature_recognition

[16] Chapran, J. (2006) Biometric Writer Identification: Feature Analysis and Classification. *International Journal of Pattern Recognition*, **20**, 483-503. https://doi.org/10.1142/S0218001406004831

[17] https://en.wikipedia.org/wiki/Convolutional_neural_network#cite_note-auto3-1