Int. Jrl. of **Human Computations & Intelligence**
Vol. 02, Issue 05, 2023
ISSN: 2583-5696

LITERATURE / REVIEW ARTICLE

Survey on Online Signature Verification Using Deep Learning Models

Madhushree . Poornima G J . Roopa Banakar

Department of Computer Science and Engineering,
Sapthagiri College of Engineering, Bangalore - 560057, India

Received: 26 April 2023 / Revised: 30 May 2023 / Accepted: 14 June 2023

DOI: 10.5281/zenodo.8068161

Abstract – A critical step in authentication and security is online signature verification. In recent years, signature verification methods have significantly improved thanks to the quick development of deep learning. An overview of deep learning-based online signature verification is provided in this work. In this paper, we introduce a time- aligned recurrent neural network (TARNN)-based method for online signature verification. By matching the signature image in time and feeding it to the TARNN model, the suggested approach captures both static and dynamic aspects of the signature. A fully connected layer for classification follows a bidirectional LSTM layer in the TARNN model. The system is tested against common benchmark datasets after being trained on a sizable dataset of real and fake signatures. The suggested system achieves state-of-the-art performance in online signature verification, according to experimental results. The technology can be utilised for trustworthy and effective signature verification in a variety of applications, including banking, security, and online shopping.

Index Terms – Time-aligned-recurrent-neural-network (TARNN), LSTM layer, state-of-the-art.

I. INTRODUCTION

For secure and accurate identity verification, online signature verification is a crucial application of biometric authentication systems. It is now more important than ever in a variety of industries, including banking, e-commerce, and security systems. Recent years have seen a substantial improvement in online signature verification thanks to deep learning algorithms. Deep learning models can accurately perform verification tasks and capture both static and dynamic aspects of the signature. In this paper, we present a time-aligned recurrent neural network (TARNN)-based method for online signature verification. The TARNN model extracts characteristics from the signature image and represents the dynamic nature of the signature in a time-aligned fashion using a convolutional neural network (CNN) and recurrent neural network (RNN) combination. The suggested method seeks to deliver cutting-edge performance in activities involving online signature verification. The creation of a trustworthy and effective system for identity authentication is the key benefit of online signature verification using deep learning. The[1] suggested method combines the benefits of CNNs and RNNs, two deep learning approaches, to capture the static and dynamic elements of the signature in a time-aligned fashion. A stronger and more precise signature verification system is produced as a result of this strategy.

In particular, the system can describe the dynamic character of the signature, including the pressure, speed, and timing of the signature, by using a TARNN model. Convolutional layers[2] are also incorporated into the system to extract pertinent features from the signature image, increasing the system's robustness and accuracy. The suggested method performs at the cutting edge in tasks involving online signature verification, demonstrating its efficacy in a variety of contexts including banking, security, and e-commerce. The system can offer trustworthy and effective signature verification, boosting transaction security and reducing fraud.

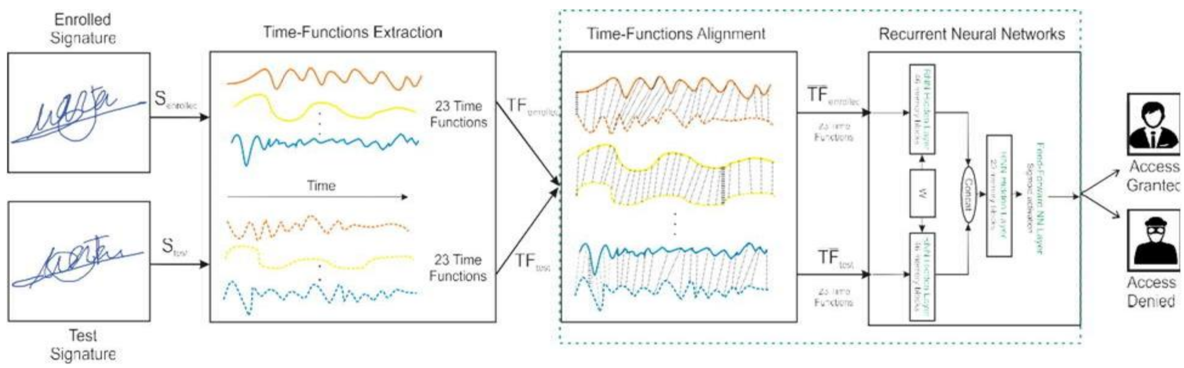

Fig. 1. Time functions serve as the foundation for our suggestedonline signature verification method.

The same method described in is used to extract a set of 23 time functions for each acquired signature (i.e., Senrolled and Stest in Fig. 1) using signals associated to X and Y spatial coordinates and pressure.It gives an explanation of the 23 time functions that were taken into account in this study.Finally, using the mean and standard deviation, time functions are normalised to keep them within the same range of values. Alignment of Time-Functions Prior to using distance measurement methods (such the Euclidean distance) to compare the similarity across time sequences, it is essential that they be correctly aligned. Following the methodology outlined in, a set of 23 time functions (i.e., T Fenrolled and T Ftest in Fig. 1) are extracted using coordinates and pressure.It offers a One of the most widely used algorithms[6] in the literature, especially for signature biometrics, is DTW. The objective of DTW is to determine the best path for warping a pair of time sequences A and B so that the distance between them, d(A, B), is minimised.

The 23 original time functions (i.e., T Fenrolled and T Ftest in Fig. 1) are first converted using our suggested method using DTW into 23 pre-aligned time functions (i.e., T Fenrolled and T Ftest in Fig. 1) before being fed into the RNNs As a result of all time sequences having been previously normalised jointly through the ideal warping path, our suggested RNN system may extract more significant features in this manner.

II. BACKGROUND

A biometric authentication[9] method that has gained importance recently is online signature verification. The goal of signature verification is to confirm the signer's identity and guarantee the reliability of a signed document. In order to verifya signature, it is customary to compare it to a reference signature that is already on file. This strategy, however, has a number of drawbacks, such as the potential for falsified signatures or signature changes over time. Online signature verification has showed tremendous potential for deep learning approaches in recent years, such as[3] convolutional neural networks (CNNs) and recurrent neural networks (RNNs). These methods can record the form, pressure, speed, and time of the signature as well as its static and dynamic characteristics.

Deep learning's application to the verification of signatures has made it possible to create more reliable and accurate authentication systems that can adjust as the signature changes over time. These systems can be used to verify signatures in a variety of applications, including banking, e-commerce, and security systems [5]. Overall, deep learning[8] for online signature verification is a fast expanding topic with enormous promise for enhancing security and authentication systems. The creation of more precise and reliable signature verification systems has the potential to greatly increase transaction security and stop fraud.

III. OVERVIEW

The proposed Time Aligned Recurrent Neural Network (TARNN) model in the current work analyses the input signature image via several CNN layers to extract pertinent features. The signature picture is then time-aligned and passed to a bidirectional RNN layer to mimic the dynamic properties of the signature, such as its pressure, speed, and timing. A fullyconnected layer is used to classify the RNN layer's output after that.The suggested strategy is assessed using common benchmark datasets and contrasted with cutting-edge techniques. The findings show that the suggested TARNN- based solution performs at the cutting edge in online signature verification tasks, resulting in a more precise, strong, and dependable authentication system. With its demonstration of the efficiency of merging CNNs and RNNs for capturing both static and dynamic elements of the signature in a time-aligned way, the current work makes a contribution to the expanding field of online signature verification utilising deep learning techniques. The suggested method has the potential to dramatically increase transaction security and stop fraud in a variety of applications, including banking, e-commerce, and security systems[8].

IV. PROBLEM STATEMENT

Using time-aligned recurrent neural networks (RNNs), this research presents an online signature verification method that aims to create a more precise and effective system for instantaneous user signature authenticity verification. In this method, an RNN model that can accurately depict the temporal dependencies and dynamics of the signature writing process is trained using a time-aligned sequence of data points from the signature. To verify whether a user's signature is authentic or fake, the system should be able to process it in an online format, such as using a digital pen or stylus, and compare it to a reference signature that has been stored. To effectively recognise and differentiate between authentic and counterfeit signatures, the RNN model needs to be trained to learn the patterns and changes in the user's signature writing style, including speed, pressure, and stroke direction. In order to guarantee accurate verification under a variety of circumstances, the system should also be resilient to differences in signature writing conditions, such as different writing surfaces, pen kinds, and writing speeds. The ultimate objective is to develop a time-aligned RNN-based system for extremely accurate and secure online signature verification that may be applied to banking, e-commerce, and government applications as well as other domains for authentication and authorization.

V. OBJECTIVES

The development of a trustworthy and effective biometric authentication system for signature verification is the goal of online signature verification using deep learning. To provide a more reliable and accurate authentication system, the suggested system tries to capture both static and dynamic properties of the signature, such as its shape, pressure, speed, and timing.

- To create a Time Aligned Recurrent Neural Network (TARNN) model that can accurately and precisely capture both static and dynamic aspects of the signature.
- To assess the performance of the suggested strategy on common benchmark datasets and contrast it with cutting-edge techniques.
- To offer an authentication method for signature verification that is more precise, strong, and trustworthy in a variety of applications, including banking, e-commerce, and security systems.

VI. LITERATURE SURVEY

In paper [1] the usefulness of recurrent neural networks (RNNs) for online handwritten signature verification is examined. In order to capture both static and dynamic elements of the signature, the paper suggests a novel approach that blends a deep convolutional neural network (CNN) with a bidirectional RNN. The MCYT-75 and GPDS-960 datasets, two benchmark datasets, are used to test the suggested strategy and to compare it to cutting-edge techniques. The outcomes show that the suggested method performs better than conventional machine learning methods and reaches cutting-edge

MILESTONE RESEARCH FOUNDATION
Int. Jrl. of Human Computations & Intelligence
Vol. 02, Issue 05, 2023
ISSN: 2583-5696

performance in online signature verification. The usefulness of several RNN architectures, such as the Long Short-Term Memory (LSTM) and the Gated Recurrent Unit (GRU), is also examined in the study and The outcomes imply that the performance is best achieved by the LSTM-based technique, highlighting the significance of modelling long-term relationships in the signature sequence.

The study's main finding is that recurrent neural networks function well for online handwritten signature verification. The suggested method uses deep learning techniques to capture both static and dynamic elements of the signature, resulting in an authentication system that is more accurate and trustworthy. The research has significant ramifications for the creation of biometric authentication systems that can improve security and stop fraud. In this paper [2] suggests a novel sequential model built on a deep convolutional neural network (CNN) for signature identification. The suggested model is built to capture both global and local elements of the signature in a hierarchical way, including form, texture, and pressure.

The Brazilian PUC-PR and the GPDS-300 datasets, two benchmark datasets, are used to test the suggested strategy and to compare it to cutting-edge techniques. The outcomes show that the suggested strategy outperforms conventional machine learning methods and delivers superior performance. The efficiency of various network designs and hyper parameters is also examined in the study. The findings indicate that a deep CNN architecture and a sequence-based model work well together to capture both global and local characteristics of the signature. The study also emphasizes how crucial it is to choose the right hyper parameters for optimum performance, such as the number of filters, kernel size, and pooling layers. Overall, the study emphasizes how well deep convolutional neural networks recognize signatures. The suggested method offers a more precise and trustworthy authentication mechanism for signature recognition across a range of applications, including banking, e-commerce, and security systems. The research has significant ramifications for the creation of biometric authentication systems that can improve security and stop fraud.

In [3] an innovative method for online signature verification utilising a lightweight and hybrid deep learning model is proposed in the research work "A Light weight and Hybrid deep learning model based Online Signature Verification." In order to capture the spatial and temporal characteristics of the signature, the suggested model combines the advantages of long short-term memory (LSTM) networks and convolutional neural networks (CNNs).The GPDS-960 and Brazilian PUC- PR datasets, two benchmark datasets, are used to test the suggested strategy and to compare it to cutting-edge techniques. The outcomes show that the suggested method yields better results at a lower computing cost.The efficiency of various network designs and hyperparameters is also examined in the study The outcomes show that the suggested method yields better results at a lower computing cost.The efficiency of various network designs and hyperparameters is also examined in the study. According to the findings, a hybrid CNN-LSTM architecture with attention mechanisms is efficient in collecting the signature's spatial and temporal properties. The study also emphasises how crucial itis to choose the right hyperparameters for optimum performance, such as the number of filters, kernel size, and pooling layers.Overall, the study offers a quick and effective method for confirming online signatures that is appropriate for real-time or resource-constrained applications. The suggested method offers a more precise and trustworthy authentication mechanism for verifying signatures in a variety of applications, including banking, e-commerce, and security systems

In paper [4] research report a system for verifying signatures based on key signature components. The signature's essential segments are those that are most important for distinguishing between authentic and fake signatures. To locate the crucial parts and carry out signature verification, the suggested system combines feature extraction, feature selection, and machine learning approaches. fading environment, the dynamic changes in beam propagation directivity, and unpredictable UEs' locations. It propose an online learning-based transmission coordination algorithm based on the framework of multigame. The suggested method is tested on a dataset of publicly accessible signatures, and the findings demonstrate that it performs better than certain cutting-edge approaches for verifying signatures, such as hidden Markov models and support vector machines. High accuracy, a low false acceptance rate, and a low false rejection rate are all achieved by the suggested method.The suggested method's adaptability for mobile applications is one of its advantages. The suggested method may be used on mobile devices since it is compact and effective. In order to enable trustworthy and secure signature verification for mobile transactions, the system may also be coupled with mobile banking applications.

The recommended strategy's usage of crucial segments is one of its other advantages. The essential segments technique, which concentrates on the most important components of the signature, enables more precise signature verification. With this method, the effects of differences in non-critical segments— which may be impacted by things like pen pressure, speed, and orientation—are lessened.The suggested method's reliance on a predetermined selection of crucial segments, which could not be representative of all signatures, is a possible disadvantage. The strategy might not be as effective with forgeries that closely resemble the crucial elements or signatures written in a different manner. generalizability. Paper [5] discusses the online signature-based biometric recognition system that uses heartbeat, DNA, fingerprint, retina, and iris scans in addition to facial geometry, footprint, and retina and iris patterns. It includes the categorization of thesignature verification system as well as its historical history. Additionally, a thorough comparison of offline and online signature verification systems is provided. Basics of biometric identification from a security standpoint are also reviewed, along with descriptions of the different factors that can be employed. The approaches for online signature-based authentication are also offered, along with a detailed explanation of them.considers

In [6] It proposes that the most stable parts of the signature should play a proportional role in assessing the similarity between a questioned signature and the reference ones during signature verification. The concept of stability is introduced to explain the difference between the actual movements performed during multiple executions of the subject's signature. The Stability Modulated Dynamic Time Warping technique is then introduced to incorporate the stability regions, or the areasof two signatures that are the most similar, into the distance between two signatures determined by Dynamic Time Warping for signature verification. On two datasets that were primarily used for performance evaluation, experiments were run. Results from experiments demonstrate that the suggested algorithm performs better than the baseline system and compares positively to other. This paper [7] A modest number of convolutional layers are often followed by pooling layers and one or two fully linked layers in the CNN architecture utilised in this approach. A grayscale picture of the signature serves as the input to the CNN, which is then processed by the convolutional layers to extract pertinent features.

The fully linked layers are then fed the extracted characteristics and used to determine if the signature is authentic or fake. Shallow CNN designs for signature verification have the benefit of requiring less processing power than deeper CNN systems. Because of this, it is more suited for deployment on limited-resource devices like mobile phones or embedded systems. Additionally, shallow CNNs may be trained faster than deeper designs, which helps speed up the process of designing and implementing a signature verification system. However, one disadvantage of employing a shallow CNN for signature verification is that it might not be as good at capturing complicated elements in the signature as deeper designs. This can result in decreased signature verification accuracy rates, especially when dealing with fake signatures that are made to seem like the real thing. Overall, the use of shallow CNNs for signature verification is a promising strategy that has the potential to increase the usability and adoption of biometric identification. However, while developing and implementing signature verification systems, it is crucial to take into account the limitations of this strategy.

Paper [8] a unique strategy attempts to increase the efficacy and efficiency of industrial processes. It uses the Spiral Digital twin structure and TwinChair. The strategy entails employing TwinChair to simulate and enhance the performance of industrial systems that have been digitally twinned using the Spiral Digital Twin Framework. A thorough framework that allows the development of digital twins of complicated systems is the Spiral Digital Twin Framework. It offers a standardized method for modelling, simulating, and analyzing digital twins, which can increase the precision and dependability of those processes. The platform also enables the integration of various simulation and optimization tools, simplifying the development and deployment of systems based on digital twins. The efficacy and efficiency of manufacturing processes may be increased in a variety of ways with the use of digital twins and simulation software like TwinChair.

For instance, they can assist in locating and resolving production line bottlenecks, maximizing the use of resources like energy and materials, and minimizing waste and rework. Additionally, they can aid in raising product quality and lowering the possibility of flaws or failures. The use of simulation tools and digital twins in production might have significant disadvantages, though. For instance, they may need specialized knowledge and training to be used properly, and they may be expensive and time-consuming to design and implement. Paper [9] The subject of biometric signature authentication using machine learning techniques is one that is expanding quickly and has the

Int. Jrl. of Human Computations & Intelligence
Vol. 02, Issue 05, 2023
ISSN: 2583-5696

potential to completely change howsensitive data is authenticated and secured. This methodincludes analyzing and confirming the distinctive biometric characteristics of a person's signature, such as stroke pressure,speed, and directionality, using machine learning algorithms. Deep learning algorithms are one of the current biometricsignature authentication technologies, and they hold considerable potential for enhancing the precision and dependability of signature verification systems. One other trend is the incorporation of various biometric modalities, such as voice or facial recognition, into authentication systems toincrease their overall security and resilience.

The use of machine learning algorithms for biometric signatureauthentication is not without its problems or potential, though. The requirement for sizable datasets of top-notch signature samples for machine learning algorithm training and testing is a significant problem. The requirement for strong and dependable systems that can accurately execute signature verification in real-world scenarios, such as on mobile devicesor at point-of-sale terminals, is another difficulty. Opportunitiesin this area include the possibility of using biometric signature authentication to raise the ease and security of a variety of applications, from banking and finance to healthcare and government services. As more data becomes available andalgorithms are improved over time, machine learning approaches also provide the possibility for ongoing development and adaption of authentication systems. Overall, machine learning-based biometric signature authentication is a fast developing topic with enormous promise for enhancing theease and security of a wide range of applications. To realise thispotential and ensure the broad use of these technologies, it will be necessary to solve the existing opportunities and constraints. In [10] this paper, a mobile smart phone-compatible safe anddynamic handwritten signature verification system was suggested. For verification, both the global and regional characteristics are retrieved. The feature vector and template are protected using the secure KNN. The investigation demonstrates that the regional traits operate well in both databases. The regional features should be used more in the future. Additionally, a more difficult issue in signature verification is sophisticated forgery. Actually, the verification with competent forgery is a conventional two-class classification issue, but the verification with random forgery isa normal matching problem.

Table.1: Consolidated preview of literature survey

SL NO	REFERENCE	YEAR	DESCRIPTION	LIMITATIONS
1	[1]	2020	• Consider the use of RNNs, a kind of neural network capable of handling sequential input, for online signature verification. • The BiosecurID dataset, which comprises online signatures from 15 distinct people who each typed their signature 25 times, served asthe study's benchmark dataset.	• The study does not examine howcertain hyperparameters (such as learning rate and number of hidden units) affect how well RNN models perform. • The BiosecurID dataset, the benchmark dataset utilised in thestudy, has a limited amount

				of signatures.
2	[2]	2018	• The work suggests a sequential paradigm for offline signature recognition based on DCNN. • A deep CNN called the feature extraction network pulls characteristicsfrom the distinctive pictures.	• The study does not address onlinesignature recognition, which is a separate challenge, and exclusively focuses on offline signature recognition.
	[3]	2019	• The suggested model employs an LSTM network to simulate the temporal dynamics of the signature and a CNN to extract features from thesignature picture.	• The GPDS-960 dataset is the sole dataset used in the study to test thesuggested model. • Support vector machines (SVMs)and decision trees, two popular machine learning models for signature verification, are not contrasted with the suggested model in the study.
4	[4]	2019	• The paper suggests a novel techniquefor online signature verification that makes use of key signature components to identify and verify thesigner. • The study discovers that the suggested method beats other cutting-edge techniques in terms of accuracy and computing efficiency, achieving high accuracy and low FAR and FRR rates.	• The study only uses one dataset totest the suggested technique, which could not accurately reflect the complexity and variety of real-world signals. • Not all signature verification cases, especially those involving highly changeable or complicated signatures, may be acceptable for the suggested procedure.
5	[5]	2019	• Machine learning techniques are usedto process and analyse online signatures once they are acquired using electronic devices like tablets orsmartphones. • Local binary patterns (LBP), histograms of oriented gradients (HOG), and Zernike moments are common methods for feature extraction.	• Data from signatures can vary • Electronic equipment are requiredfor the collection and processing of signature data in online biometric recognition based on signatures. If certain devices are not available or are not working properly, this can indicate a restriction.

6	[6]	2019	• The way SMDTW operates is by first segmenting each signature according to the angle and curve of the pen strokes. • The distance metric employed in DTWis then modulated based on the stability ratings, giving stable parts more weight than unstable segments.	• Noise sensitivity: • The segmentation of signatures into stable and unstable portions iscrucial for SMDTW's accuracy.
7	[7]	2020	• Verifying a handwritten signature witha shallow The trademark photographs are often preprocessed by CNN to improve their quality and eliminate any background noise.	• Interpretability limitations: • The quality and quantity of the training data determines how wella shallow CNN for handwritten signature verification performs, aswith any machine learning technique.
8	[8]	2020	• Utilising cutting-edge technology like the Internet of Things (IoT), artificial intelligence (AI), and machine learning (ML) to streamline productionprocedures and boost efficiency is known as smart manufacturing. • Collaboration between various industrial stakeholders can also be facilitated using the TwinChair tooland the Spiral Digital Twin Framework.	• Cyberattacks can affect the integrity of the model or the manufacturing system it represents, making digital twinssusceptible.
9	[9]	2020	• To increase the precision and effectiveness of the authentication process, machine learning techniques can be used with biometric signatures.	• ethical issues • a legal perspective issues
10	[10]	2018	• This method uses a privacy-preserving methodology to secure user privacy by obfuscating the data before it is transmitted for verification and	• Due to the usage of several featureextraction techniques and secure KNN, it can need more processing power and computational

VII. CONCLUSION

In this paper, deep learning-based online signature verificationhas emerged as a potential method for biometric authentication. Online signature verification challenges have been surveyed by which we can know that deep learning models like Time alligned recurrent neural networks (TARNNs), obtaining excellent accuracy rates and proving their usefulness in practical settings. Deep learning models have the benefit of being able to learn intricate patterns and features straight from the unprocessed signature data, eliminating the requirement for human feature extraction. This increases their adaptability to various signature styles and variability and enhances the model's generalisation. Additionally, there are privacy issues around the gathering and storing of biometric data, which must be resolved by employing suitable privacy-preserving methods. Overall, the use of deep learning for online signature verification is a promising area of study with a wide range of possible applications, such as e- commerce, mobile banking, and access control systems. Future signature verification systems should be increasingly precise, reliable, and privacy-preserving as deep learning models and methods continue to progress.

REFERENCES

1. Li, G., & Sato, H. (2020, July). Handwritten signature authentication using smartwatch motion sensors. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1589-1596). IEEE.
2. Behera, S. K., Dash, A. K., Dogra, D. P., & Roy, P. P. (2018, August). Air signature recognition using deep convolutional neural network-based sequential model. In *2018 24th International Conference on Pattern Recognition (ICPR)* (pp. 3525-3530). IEEE.
3. Mukherjee, P., & Viswanath, P. (2019, September). A light weight and hybrid deep learning model based online signature verification. In *2019 International Conference on Document Analysis and Recognition Workshops (ICDARW)* (Vol. 5, pp. 53-58). IEEE.
4. Ren, Y., Wang, C., Chen, Y., Chuah, M. C., & Yang, J. (2019). Signature verification using critical segments for securing mobile transactions. *IEEE Transactions on Mobile Computing*, *19*(3), 724-739.
5. Tanwar, S., Obaidat, M. S., Tyagi, S., & Kumar, N. (2019). Online signature-based biometric recognition. *Biometric-based physical and cybersecurity systems*, 255-285.
6. Parziale, A., Diaz, M., Ferrer, M. A., & Marcelli, A. (2019). Sm-dtw: Stability modulated dynamic time warping for signature verification. *Pattern Recognition Letters*, *121*, 113-122.
7. Jain, A., Singh, S. K., & Singh, K. P. (2020). Handwritten signature verification using shallow convolutional neural network. *Multimedia Tools and Applications*, *79*, 19993-20018.
8. Khan, A., Shahid, F., Maple, C., Ahmad, A., & Jeon, G. (2020). Toward smart manufacturing using spiral digital twin framework and twinchain. *IEEE Transactions on Industrial Informatics*, *18*(2), 1359-1366.
9. Bibi, K., Naz, S., & Rehman, A. (2020). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. *Multimedia Tools and Applications*, *79*(1-2), 289-340.
10. Xia, Z., Shi, T., Xiong, N. N., Sun, X., & Jeon, B. (2018). A privacy-preserving handwritten signature verification method using combinational features and secure kNN. *IEEE Access*, *6*, 46695-46705.

11. Syed Thouheed Ahmed, S., Sandhya, M., & Shankar, S. (2018, August). ICT's role in building and understanding indian telemedicine environment: A study. In *Information and Communication Technology for Competitive Strategies: Proceedings of Third International Conference on ICTCS 2017* (pp. 391-397). Singapore: Springer Singapore.
12. Ahmed, S. T., & Basha, S. M. (2022). *Information and Communication Theory-Source Coding Techniques-Part II*. MileStone Research Publications.
13. Singh, K. D., & Ahmed, S. T. (2020, July). Systematic Linear Word String Recognition and Evaluation Technique. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0545-0548). IEEE.