GLOBUS

Globus An International Journal of Medical Science, Engineering and Technology
A Refereed Research Journal
Vol 10 / No 2 / Jul-Dec 2021 ISSN: 2319-8958

ARTIFICIAL NEURAL NETWORKS TO ENHANCE SECURITY SYSTEMS

*Pratap Chandra Mishra

**Dr Rajesh Keshavrao Deshmukh

Paper Received: 14.11.2021 / **Paper Accepted**: 06.12.2021 / **Paper Published**: 08.12.2021
Corresponding Author: Pratap Chandra Mishra; doi:10.46360/globus.met.320212021

Abstract

Artificial Neural Networks (ANNs) have become extremely effective tools for improving security systems in a variety of industries. Artificial neural networks (ANNs) possess the capacity to learn and adapt from data, allowing them to precisely identify abnormalities, anticipate risks, and discern odd patterns. The integration of ANNs into security systems is covered in this abstract, with particular attention paid to the use of ANNs in biometric authentication, cybersecurity, and surveillance. It emphasizes how ANNs may boost overall security architecture by increasing detection rates and decreasing false positives. The study also examines issues like the necessity for large training datasets, data privacy problems, and the possibility of adversarial assaults. Future thoughts on the creation of more robust ANN-based security systems that are better able to adjust to the dynamic nature of security threats are included in the conclusion. The present study highlights the remarkable capacity of neural networks to enhance security measures by augmenting their intelligence and responsiveness to novel threats.

Keywords: Artificial Neural Network, ANN, Services, Security, Network, System.

Introduction

Unlike inference or rule-based approaches, neural networks rely on their ability to recognize patterns based on past performance. Although they are most commonly used in adaptive systems for pattern recognition, neural networks can be used to solve a wide range of other problems. A choice scenario can be reduced to a pattern recognition problem with little effort. Neural networks have been applied by many researchers to business decision-making scenarios in earlier studies.

To solve the building modularization difficulty, the authors have developed and implemented a multi-layered self-organizing neural network for classification purposes. Two neural network paradigms are used in the multilayered network: competitive learning and Kohonen's self-organizing feature maps. These two paradigms use mostly unsupervised learning techniques. The goal of unsupervised learning techniques is to change the weights so that sufficiently similar input vectors produce equal output vectors. Kohonen has created self-organizing maps and utilized them for signal processing and pattern recognition tasks. These maps often classify a pattern represented by a vector of values, where each vector element is associated with a pattern element.

Although some iterations of Kohonen's approach might include some degree of supervision, the strategy primarily depends on an unsupervised learning technique. Kohonen's method has the advantage of having a simple computational framework. This makes it possible for it to function as a credible neural model and to be effectively used for tasks including speech recognition, image processing, pattern identification, control tasks, and robot motor learning. In a number of publications, Kohonen has shown the technique's effectiveness through the presentation of mathematical reasons and computer simulation results.

Literature Review

Mouss (2019) [1] The extraction of features and the application of classification methods are crucial stages in a recognition system. An effective classifier and feature extraction are crucial components in a recognition system for enhancing the recognition rate.

*Research Scholar, Kalinga University, Naya Raipur, Chhattisgarh, India.
**Supervisor, Kalinga University, Naya Raipur, Chhattisgarh, India.

This study presents a novel technique aimed at accurately identifying the ten digits of printed Arabic numerals, which are widely used as the primary symbolic representation of numbers worldwide. This study utilized Hu moments, number of holes, and surface area as features that are robust to geometric changes. Seven distinct classifiers were employed: Naive Bayesian, Multi-Layer Perceptron (MLP), Linear Discriminant Analysis (LDA), and Pseudo-Inverse. The machine learning algorithms used are Support Vector Machine (SVM), Decision Tree, and K-Nearest Neighbor (KNN). The consideration of classifier combination is being discussed. Empirical experiments have proven that our methodology yields favorable outcomes when applied to a diverse range of printed digits, encompassing various fonts and sizes. The objective of this research study is to create a system that can accurately identify printed digits. A highly researched area in the field of pattern recognition as well as machine learning is the fusion of multiple classifiers. This approach leverages the individual strengths of classifiers while compensating for their individual weaknesses, and has demonstrated its effectiveness in combining results from different classifiers. The suggested system employs many classifiers, including KNN, SVM, decision tree, pseudo inverse, LDA, Naive Bayesian, and MLP, to accurately identify printed digits. The Hu moments features, which are robust to geometric changes such as translation, scaling, and rotation, were retrieved and enhanced by considering the number of holes, surface area, and enclosed cavity of the digit. Recent studies have lacked sufficient research on the recognition of multi-font & multi-size digits, specifically in relation to experimental testing conducted on printed digits. The data unequivocally illustrate the efficacy of the proposed strategy. In this endeavor, we have endeavored to amalgamate the decisions of classifiers in order to accomplish recognition.

Pal et al. (2014) [4] conducted a comparative study on Devnagari handwritten character recognition using 12 different classifiers, including PD, subspace method (SM), linear discriminant function (LDF), SVM, MQDF, mirror image learning (MIL), Euclidean distance (ED), nearest neighbor, KNN, modified PD (MPD), compound PD (CPD), and compound MQDF (CMQDF). Based on the experiment, it was seen that the MIL classifier yielded the most favorable outcomes, while the ED classifier exhibited the least favorable findings out of the 12 classifiers that were evaluated. The system underwent testing using 36,172 samples and achieved a recognition accuracy of 95.19%.

Analysis

Neural networks with a feed forward multilayered network structure are typically referred to as competitive learning systems. Neurons compete with one another to activate in response to randomly chosen input patterns. The neuron with the weight vector that is closest to the random pattern in Euclidean distance at the end of each iteration is deemed the winner. A single output neuron is always active thanks to competitive learning. 'Winner-take-all' refers to the fact that output neurons fight to be the ones that fire. Competitive learning networks aim to categorize or organize the input data. Similar inputs are put in the same category and ought to activate the same cell as a result. Since competitive learning is inherently unsupervised, the classes must be found by the network on its own using the correlations found in the input data. Feature mapping stated earlier is closely linked to competitive learning.

Artificial intelligence (AI), especially with neural networks, offers significant advancements in enhancing security systems in various fields. The use of sophisticated, accurate, and automated security measures is made possible by this integration. An extensive examination of the use of neural networks to improve security frameworks is provided below:

1. Identifying Faces and Biometrics

Neural networks are commonly employed in the security industry for facial recognition technology. Neural networks are trained extensively on big facial picture datasets so that these systems may learn to recognize certain facial features and identify patterns. This feature is used by security systems for a number of applications, such as controlling access to buildings, airports, and other extremely secure locations, as well as for observation and monitoring needs. Neural networks enhance fingerprint analysis and iris identification in addition to facial recognition, resulting in a multi-layered security system that is highly impervious to unwanted access.

2. Finding Anomalies

Pattern recognition is one area in which neural networks thrive. Their abilities to learn about normal network behavior and spot deviations that can point to a security issue, such malware or a network incursion, making them ideal for spotting anomalies in network security. In IT infrastructures, this program is crucial for ensuring data integrity and minimizing data breaches.

3. Identifying Fraud

In the financial services industry, neural networks enhance security protocols by detecting and signaling instances of fraudulent activity. Artificial intelligence (AI) systems are capable of quickly spotting possible fraud by analyzing expenditure patterns and comparing them to known fraudulent

activity. This makes it possible to identify unusual transactions quickly, thus cutting down on the amount of time needed to find fraudulent activity and lowering the frequency of false positives that annoy users.

4. Expected Protection

Neural networks can predict potential security threats by looking at long-term patterns and trends. Artificial intelligence in the field of cybersecurity can predict weaknesses that may be exploited in the future, even before they become active threats. This makes it possible for IT teams to patch systems or strengthen security procedures in order to proactively address these vulnerabilities. Proactive security measures are significantly more effective than traditional reactive ones.

5. Improving Security Functions

Security resource allocation can be optimized via neural networks. Artificial intelligence (AI) can be used, for example, to analyze incident trends and recommend the best locations for security personnel or cameras in physical security scenarios. In cybersecurity, artificial intelligence (AI) models can dynamically allocate resources in real-time to defend against threats that have been recognized, strengthening response strategies and optimizing resource usage.

6. Challenges and Elements to Consider

Despite the benefits, there are challenges with integrating artificial intelligence and neural networks into security systems. Privacy is a very important concern, especially when it comes to cutting edge technologies like facial recognition. The reliance on high-quality data raises further questions. High-quality data is the only way neural networks can be trained to function well. Inadequate data in security applications can lead to errors and biases. In addition, these systems require ongoing maintenance and retraining to adapt to evolving threats and changing environments.

One noteworthy and remarkable development in the field of security is the incorporation of artificial intelligence (AI) including neural networks into security systems. By automating the identification and reaction processes, increasing accuracy, and enabling proactive security measures, neural networks significantly improve security systems.

However, it's imperative to find a compromise among these benefits and the requirements to protect privacy, make sure technology is used ethically, and modify AI capabilities to counteract changing threats. These technologies are expected to play a more central role in security as they develop, influencing developments in both the physical & cybersecurity realms.

Conclusion

The security system environment is changing due to Artificial Neural Networks (ANNs), which provide advanced solutions that improve operational efficiency and detection capabilities. Artificial neural networks (ANNs) have shown great promise in detecting intricate patterns and abnormalities that may defy conventional security measures due to their capacity to process and learn from enormous volumes of data. The use of ANNs in surveillance, biometric authentication, and cybersecurity has greatly improved security systems' capacity to anticipate attacks and react to them more precisely. Future research and development must, however, focus on issues like protecting against adversarial attacks and guaranteeing data privacy. Future developments in neural network technology and their incorporation into security frameworks should significantly improve security systems' dependability and efficacy while also increasing their capacity to respond to changing threat environments.

Artificial intelligence (AI) refers to the capacity of artificial entities, such as computers or other gadgets, to effectively address complex issues. Intelligence can be understood as the computational aspect of the ability to do tasks in the real world, whereas artificial intelligence is the combination of computer science and physiology. Intelligence encompasses the abilities to engage in reasoning, envisioning, inventing, recalling, comprehending, identifying patterns, making judgments, adapting to change, and learning from experience. The objective of artificial intelligence is to enable computers to exhibit behavior similar to that of humans. Artificial intelligence endeavors to address complex problems in a manner that is more compassionate and considerate than humans. Consequently, it is commonly known as artificial intelligence. Artificial Intelligence (AI) can be categorized into two main types: strong AI and weak AI.

Strong AI posits that machines can achieve the ability to reason by representing future human notions. Strong AI asserts that in the near future, we will be surrounded by machines that exhibit human-like behavior and possess intelligence on par with humans. If this is the case, then these machines will possess the ability to engage in logical thinking, cognitive processing, and perform all the functions that humans are capable of. There is a contemporary debate regarding the feasibility of creating highly advanced artificial intelligence, however current research is still distant from achieving this goal.

The fundamental concept behind NAI is that it enables robots to exhibit intelligent behavior. Weak AI posits that it is relatively easy to imbue computers with cognitive capacities, hence

enhancing their efficacy as tools - and this phenomenon is already underway. For example, a human chess player may perceive the computer's moves as remarkable while playing chess against it. Nevertheless, the act of applying chess does not involve any form of preparation or thought. By pre-programming each action into the computer, a person ensures that the software executes the correct motion at the precise moment. Expert witness systems, telex vehicles, and speech recognition systems are more examples of inadequate artificial intelligence.

An extension of mathematical models used to represent biological nerve systems is artificial neural networks (ANN). ANNs are composed of simple clusters of processors known as "neurons," each of which may possess localized memory. These units only utilize the inputs they get through unidirectional connections or linkages, as well as their local data. A network element possesses a regulation that combines the incoming signals and another regulation that calculates the outgoing signals and transmits them to other network components. Callen uses the term "activation function" to describe the formula used for calculating the output. A neural network's structure consists of three layers. The input layer is the uppermost layer that directly interacts with the external environment. The hidden units, located in the second layer, do computations using the provided function. Lastly, the output layer, situated at the top, is responsible for generating the final output.

The synaptic weights between neurons function as the storage mechanism for knowledge in neural networks. The network propagates input data from one layer to the next until output data is generated. If the output of a multilayer perceptron with a backpropagation algorithm differs from the intended output, the error is calculated and propagated back through the network. Errors propagate and impact synaptic weights. Presently, Days researchers are endeavoring to construct an electronic network on silicon that emulates the structure and functioning of the human brain. The primary characteristic that makes artificial neural networks (ANNs) a powerful tool is their universality. The process by which the human brain acquires the capacity to identify patterns and store them for future use. Similarly, neural networks that have undergone appropriate development have the ability to remember and acquire patterns.

Conflicts of Interest Disclosure

The authors declare that there are no significant competing financial, professional, or personal interests that might have influenced the performance or presentation of the work described in this manuscript.

References

1. Khedidja, Derdour & Hayet, Mouss (2019). Multiple Classifiers and Invariant Features Extraction for Digit Recognition. International Journal of Computer and Electrical Engineering, 11, 41-52. 10.17706/IJCEE.2019.11.1.41-52.
2. Arora, Amit & et al. (2011). Machine recognition of Devnagari script. IEEE Transaction Systems Man Cybernetics, 9(45), 435-441.
3. Kumar, Sunil (2013). Fine classification & recognition of hand written Devnagari characters with regular expressions & minimum edit distance method. Journal of computers, 3(5), 11-17.
4. Pal, Sangeeta & et al. (2014). A Two Stage Classification Approach for Handwritten Devnagari Characters. IEEE International Conference on Computational Intelligence and Multimedia Applications, 399-403.
5. Mukherjee, Rege (2015). Recognition of non-compound handwritten Devnagari characters using a combination of MLP and minimum edit distance. International Journal Computer Science Security, 4(1), 107-120.