ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (47-53), Month: January - March 2020, Available at: www.researchpublish.com

SECURITY ANALYSIS IN CONVOLUTIONAL NEURAL NETWORK USING TIME SERIES CLASSIFICATION AND CRYPTO SCHEMES

[1]S.KAVITHA, [2]A.SENTHILKUMAR

[1]Research scholar, Dept. of. Computer science, Tamil University, Thanjavur-613010.

[2]Asst.professor, Dept. of .Computer Science,Tamil University (Established by the Govt.of.Tamilnadu),Thanjavur-613010

Abstract: **For image based analysis in network implications, an important verified visual representation are applied which are termed as, 'Convolution Neural Networks'. The existing Convolution Neural Networks process involves , 'Time Series Classification' were an image depicted as the data set are predicted to extract a pattern. Based on this pattern, exact specification to predict a concrete solution are allowed in the existing schemes. To enhance the existing system and to propose novelty in adapting the information security process. The existing system is adapted to undergo the process of appending secrecy bits in the original image are executed in this work. Further the secret pattern orientated image are transmitted to all other participating nodes, which ensures a secured transmission in the networks. After the quantization analysis of the existing models the secrecy image representation has produced considerably significant percentage of 5% increased protection measures with respect to its dataset image representation. Hence the proposed system evaluates the time series classification that are commonly used in Convolution Neural Networks and adopts security enhancement which proves that data are transmitted in a secured manner by utilizing the cryptography methods.**

Keywords: **Neural Network,, Cryptography , Information security .**

1. INTRODUCTION

Convolutional Neural Networks (CNNs) have been established as a robust class of models for image recognition problems. Encouraged by these results, we provide an extensive empirical evaluation of CNNs on large-scale video classification using a new dataset of 1 million YouTube videos belonging to 487 classes. We study multiple approaches for extending the connectivity of a CNN in time domain to take advantage of local spatio-temporal information and suggest a multiresolution, forested architecture as a promising way of speeding up the training. Our best spatio-temporal networks display significant performance improvements compared to strong feature-based baselines (55.3% to 63.9%), but only a surprisingly modest improvement compared to single-frame models (59.3% to 60.9%). We further study the generalization performance of our best model by retraining the top layers on the Action Recognition dataset and observe significant performance improvements compared to the UCF-101 baseline model. The system introduces a class of efficient models called Mobile Nets for mobile and embedded vision applications. Mobile Nets are based on a streamlined architecture that uses depth-wise separable convolutions to build light weight in deep neural networks. We introduce two simple global hyper-parameters that efficiently trade off between latency and accuracy. These hyper-parameters allow the model builder to choose the right sized model for their application based on the constraints of the problem. We present extensive experiments on resource and accuracy tradeoffs and show strong performance compared to other popular models on Image Net classification. The effectiveness of Mobile Nets known across a wide range of applications are considered as an example and use cases including object detection, fine grain classification, face attributes and large scale geo-localization. Rendering the semantic content of an image in different styles is a difficult image processing task.

Arguably, a major limiting factor for previous approaches has been the lack of image representations that explicitly represent semantic information and, thus, allow separating image content from style. Here the use of image representations are derived from Convolutional Neural Networks optimised for object recognition, which make high level image information explicit. Further the system introduces Neural Algorithm of Artistic Style that can separate and recombine the image content and style of natural images. The algorithm allows us to produce new images of high perceptual quality that combine the content of an arbitrary photograph with the appearance of numerous well known artworks. Our results provide new insights into the deep image representations learned by Convolutional Neural Networks and demonstrate their potential for high level image synthesis and manipulation. As a successful deep model applied in image super-resolution (SR), the Super-Resolution Convolutional Neural Network (SRCNN) has demonstrated superior performance to the previous hand-crafted models either in speed and restoration quality. How ever, the high computational cost still hinders it from practical usage that demands real-time performance (24 fps). The aim of accelerating the current SRCNN, and propose a compact hourglass-shape CNN structure for faster and better SR. Redesigning the SRCNN structure mainly in three aspects.

First, we introduce a deconvolution layer at the end of the network, then the mapping is learned directly from the original low-resolution image (without interpolation) to the high-resolution one. Secondly, reformulating the mapping layer by shrinking the input feature dimension before mapping and expanding back afterwards. Third, we adopt smaller filter sizes but more mapping layers. The proposed model achieves a speed up of more than 40 times with even superior restoration quality. Further, in order to present the parameter settings that can achieve real-time performance on a generic CPU while still maintaining good performance. A corresponding transfer strategy is also proposed for fast training and testing across different upscaling factors. The ability to accurately represent sentences is central to language understanding. We describe a convolutional architecture dubbed the Dynamic Convolutional Neural Network (DCNN) that may adopt for the semantic modelling of sentences. The network uses Dynamic k-Max Pooling, a global pooling operation over linear sequences. The network handles input sentences of varying length and induces a feature graph over the sentence that is capable of explicitly capturing short and long-range relations.

The network does not rely on a parse tree and is easily applicable to any language. Testing the DCNN in four experiments: small scale binary and multi-class sentiment prediction, six-way question classification and Twitter sentiment prediction by distant supervision. The network achieves excellent performance in the first three tasks and a greater than 25% error reduction in the last task with respect to the strongest baseline. MatConvNet is an open source implementation of Convolutional Neural Networks (CNNs) with a deep integration in the MATLAB environment. The toolbox is designed with an emphasis on simplicity and flexibility. It exposes the building blocks of CNNs as easy-to-use MATLAB functions, providing routines for computing convolutions with filter banks, feature pooling, normalisation, and much more. MatConvNet can be easily extended, often using only MATLAB code, allowing fast prototyping of new CNN architectures. At the same time, it supports efficient computation on CPU and GPU, allowing to train complex models on large datasets such as ImageNet ILSVRC containing millions of training examples. A successful matching algorithm needs to adequately model the internal structures of language objects and the interaction betweeen them. As a step toward this goal, we propose convolutional neural network models for matching two sentences, by adapting the convolutional strategy in vision and speech. The proposed models not only nicely represent the hierarchical structures of sentences with their layer-by-layer composition and pooling, but also capture the rich matching patterns at different levels. Our models are rather generic, requiring no prior knowledge on language, and can hence be applied to matching tasks of different nature and in different languages. The empirical study on a variety of matching tasks demonstrates the efficacy of the proposed model on a variety of matching tasks and its superiority to competitor models. We trained a large, deep convolutional neural network to classify the 1.2 million high-resolution images in the ImageNet LSVRC-2010 contest into the 1000 different classes. On the test data, we achieved top-1 and top-5 error rates of 37.5% and 17.0%, respectively, which is considerably better than

2. LITERATURE SURVEY

1. Hasim Sak et al (2014) Long Short-Term Memory (LSTM) is a specific recurrent neural network (RNN) architecture that was designed to model temporal sequences and their long-range dependencies more accurately than conventional RNNs. We explore LSTM RNN architectures for large scale acoustic modeling in speech recognition. We recently showed that LSTM RNNs are more effective than DNNs and conventional RNNs for acoustic modeling, considering moderately-sized models trained on a single machine. Here, we introduce the first distributed training of

LSTM RNNs using asynchronous stochastic gradient descent optimization on a large cluster of machines. We show that a two-layer deep LSTM RNN where each LSTM layer has a linear recurrent projection layer can exceed state-of-the-art speech recognition performance. This architecture makes more effective use of model parameters than the others considered, converges quickly, and outperforms a deep feed forward neural network having an order of magnitude more parameters.

2. Felix A. Gers et al (2002) The temporal distance between events conveys information essential for numerous sequential tasks such as motor control and rhythm detection. While Hidden Markov Models tend to ignore this information, recurrent neural networks (RNNs) can in principle learn to make use of it. We focus on Long Short-Term Memory (LSTM) because it has been shown to outperform other RNNs on tasks involving long time lags. We find that LSTM augmented by "peephole connections" from its internal cells to its multiplicative gates can learn the fine distinction between sequences of spikes spaced either 50 or 49 time steps apart without the help of any short training exemplars. Without external resets or teacher forcing, our LSTM variant also learns to generate stable streams of precisely timed spikes and other highly nonlinear periodic patterns. This makes LSTM a promising approach for tasks that require the accurate measurement or generation of time intervals.

3. Huiting Zheng et al (2017) Accurate load forecasting is an important issue for the reliable and efficient operation of a power system. This study presents a hybrid algorithm that combines similar days (SD) selection, empirical mode decomposition (EMD), and long short-term memory (LSTM) neural networks to construct a prediction model (i.e., SD-EMD-LSTM) for short-term load forecasting. The extreme gradient boosting-based weighted k-means algorithm is used to evaluate the similarity between the forecasting and historical days. The EMD method is employed to decompose the SD load to several intrinsic mode functions (IMFs) and residual. Separated LSTM neural networks were also employed to forecast each IMF and residual. Lastly, the forecasting values from each LSTM model were reconstructed. Numerical testing demonstrates that the SD-EMD-LSTM method can accurately forecast the electric load.

4. Ben Athiwaratkun et al (2017) Malicious software, or malware, continues to be a problem for computer users, corporations, and governments. Previous research has explored training file-based, malware classifiers using a two-stage approach. In the first stage, a malware language model is used to learn the feature representation which is then input to a second stage malware classifier.

5. In Pascanu et al. [1], the language model is either a standard recurrent neural network (RNN) or an echo state network (ESN). In this work, we propose several new malware classification architectures which include a long short-term memory (LSTM) language model and a gated recurrent unit (GRU) language model. We also propose using an attention mechanism similar to [12] from the machine translation literature, in addition to temporal max pooling used in [1], as an alternative way to construct the file representation from neural features. Finally, we propose a new single-stage malware classifier based on a character-level convolutional neural network (CNN). Results show that the LSTM with temporal max pooling and logistic regression offers a 31.3% improvement in the true positive rate compared to the best system in [1] at a false positive rate of 1%.

6. zen J. et al (2007) Sequential machine learning techniques allow the extraction of critical information embedded in hours of continuously monitored signals in the intensive care unit (ICU). The aim of this project was to provide clinicians with a continuous predictive probability of a patient's physiological status belonging to a range of conditions. Experimentation was done with Hidden Markov Models (HMMs), and Recurrent Neural Networks (RNNs). To date, both models have performed similarly, but more experimentation with deep RNNs is needed.

3. PROBLEM DEFINITION

Several variants of evolutionary algorithms (EAs) have been applied to solve the project scheduling problem (PSP), yet their performance highly depends on design choices for the EA. It is still unclear how and why different EAs perform differently. We present the first runtime analysis for the PSP, gaining insights into the performance of EAs on the PSP in general, and on specific instance classes that are easy or hard. Our theoretical analysis has practical implications—based on it, we derive an improved EA design. This includes normalizing employee's dedication for different tasks to ensure they are not working overtime; a fitness function that requires fewer pre-defined parameters and provides a clear gradient towards feasible solutions; and an improved representation and mutation operator. Both our theoretical and empirical results show that our design is very effective. Combining the use of normalization to a population gave the best results in

our experiments, and normalization was a key component for the practical effectiveness of the new design. Not only does our paper offer a new and effective algorithm for the PSP, it also provides a rigorous theoretical analysis to explain the efficiency of the algorithm, especially for increasingly large projects. In the previous design the PSP is particularly challenging when the project is large. The space of possible allocations of employees to tasks is enormous, and providing an optimal allocation of employees to tasks becomes a very difficult task. When allocating employees to tasks, employees can divide their attention among several tasks at the same time in the PSP. The new design includes normalization of dedication values, a tailored mutation operator, and fitness functions with a strong gradient towards feasible solutions. Normalization removes the problem of overwork and allows an EA to focus on the solution quality.

It facilitates finding the right balance between dedication values for different tasks and allows employees to adapt their workload whenever other tasks are started or finished. The new design includes normalization of dedication values, a tailored mutation operator, and fitness functions with a strong gradient towards feasible solutions. Normalization removes the problem of overwork and allows an EA to focus on the solution quality. It facilitates finding the right balance between dedication values for different tasks and allows employees to adapt their workload whenever other tasks are started or finished. It is a particularly demanding task and, being a project planning task, is vital to many software engineering activities. Its process involves several duties identify project activities; identify activity dependencies; estimate Resources for activities; allocate people to activities; and create project charts. Helps software manager in producing schedules that meet all constraints.The system provides a very useful insight into optimize objectives such as cost and completion time.

4. SYSTEM METHODOLOGY

Methodology is termed as the structured sequence of steps/procedures in order to solve a given problem. This proposed system narrats the importance of cryptographic schemes as an useful technique where it can be utilized in convolutional neural network methods thereby the time series classification is based on the timing sequences and also with the image representations, the secrecy measures are adopted along with the exsiting methods and proves the same with respect to 5 datasets. The following steps depicts the complete sequence of the proposad method as follows.Finally the image transformations are now places for secured transmissions over the networl where information security principle are achieved. Convolutional Neural Networks (CNNs) are state-of-the art models for many image and video classification tasks. However, training on large-size training samples is currently computationally impossible. Hence when the training data is multi-gigapixel images, only small patches of the original images can be used as training input. Since there is no guarantee that each patch is discriminative, we advocate the use of Multiple Instance Learning (MIL) to combine evidence from multiple patches sampled from the same image. In this paper we propose a framework that integrates MIL with CNNs. In our algorithm, patches of the images or videos are treated as instances, where only the image or video-level label is given. Our algorithm iteratively identifies discriminative patches in a high resolution image and trains a CNN on them. In the test phase, instead of using voting to the predict the label of the image, we train a logistic regression model to aggregate the patch-level predictions. Our method selects discriminative patches more robustly through the use of Gaussian smoothing.

5. SYSTEM DESIGN

To combine multiple scales, spatial relations, and multiple features, we formulate rich context models using Markov random fields. To solve the optimization problem, we analyze global and local approaches, where a top–down hierarchical algorithm has the best performance. Experimental results show that exploiting different types of contextual relations jointly consistently improves the recognition accuracy. While deep convolutional neural networks (CNNs) have shown a great success in single-label image classification, it is important to note that real world images generally contain multiple labels, which could correspond to different objects, scenes, actions and attributes in an image. Traditional approaches to multi-label image classification learn independent classifiers for each category and employ ranking or thresholding on the classification results. These techniques, although working well, fail to explicitly exploit the label dependencies in an image. In this paper, we utilize recurrent neural networks (RNNs) to address this problem. Combined with CNNs, the proposed CNN-RNN framework learns a joint image-label embedding to characterize the semantic label dependency as well as the image-label relevance, and it can be trained end-to-end from scratch to integrate both information in a unified framework. Experimental results on public benchmark datasets demonstrate that the proposed architecture achieves better performance than the state-of-the-art multi-label classification models.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 1, pp: (47-53), Month: January - March 2020, Available at: www.researchpublish.com

Convolutional Neural Networks (CNNs) are state-of-the art models for many image and video classification tasks. However, training on large-size training samples is currently computationally impossible. Hence when the training data is multi-gigapixel images, only small patches of the original images can be used as training input. Since there is no guarantee that each patch is discriminative, we advocate the use of Multiple Instance Learning (MIL) to combine evidence from multiple patches sampled from the same image. In this paper we propose a framework that integrates MIL with CNNs. In our algorithm, patches of the images or videos are treated as instances, where only the image or video-level label is given. Our algorithm iteratively identifies discriminative patches in a high resolution image and trains a CNN on them. In the test phase, instead of using voting to the predict the label of the image, we train a logistic regression model to aggregate the patch-level predictions. Our method selects discriminative patches more robustly through the use of Gaussian smoothing. We apply our method to gloomy (the most common brain cancer) subtype classification based on multi-gig pixel whole slide images (WSI) from The Cancer Genome Atlas (TCGA) dataset. We can classify Glioblastoma (GBM) and Low-Grade Glomma (LGG) with an accuracy of 97%. Furthermore, for the first time, we attempt to classify the three most common subtypes of LGG, a much more challenging task. We achieved an accuracy of 57.1% which is similar to the inter-observer agreement between experienced pathologists.

6. SYSTEM ARCHITECTURE

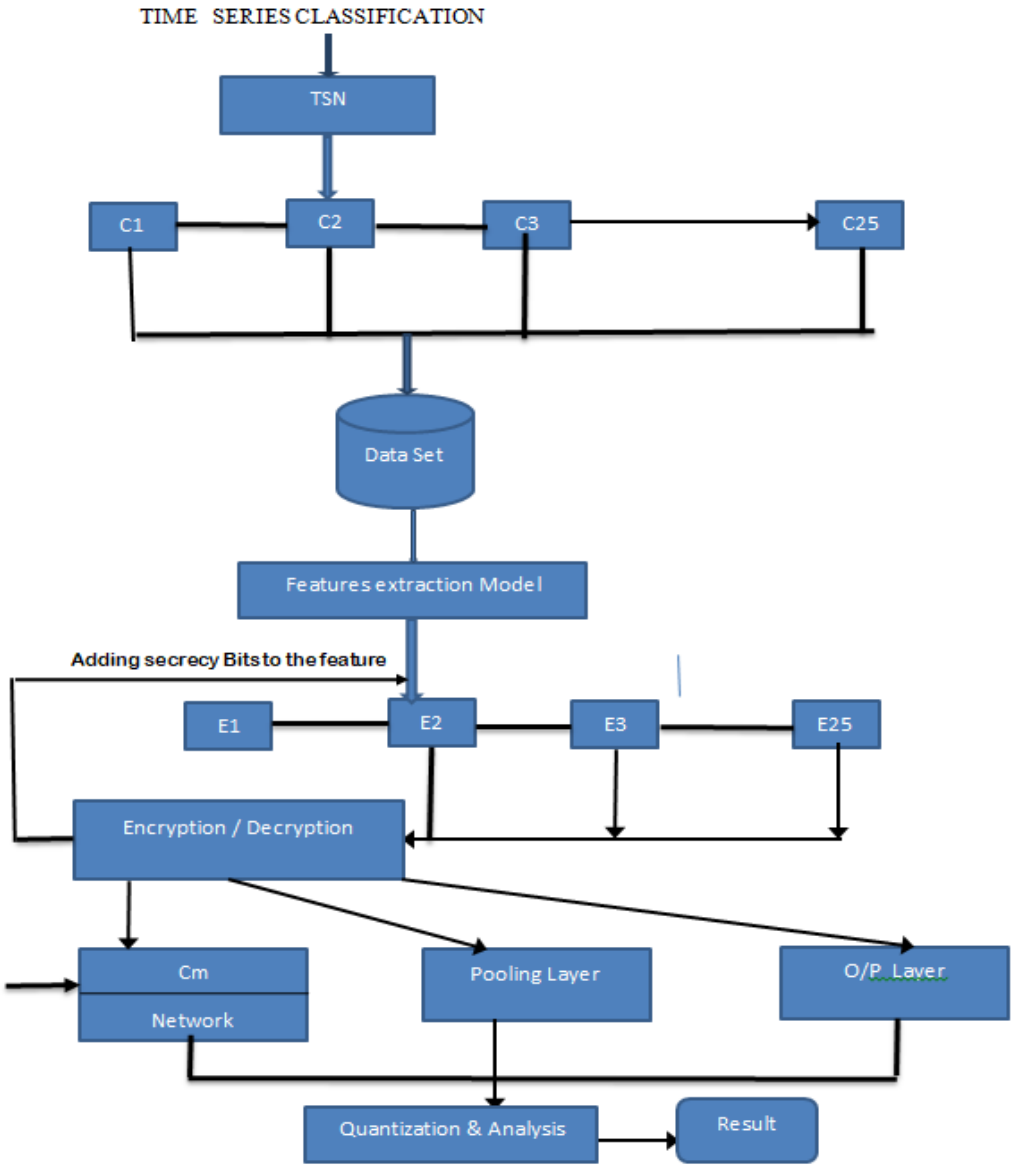

Fig 1: Security Analysis in Convolutional Neural Network

Modules

2.1 Convolution Network

2.2 The Pooling Layer

2.3 Encryption Decryption process

2.4 The Output layer

Convolutional Network

Convolutional Neural Networks are very similar to ordinary Neural Networks. They are made up of neurons that have learnable weights and biases. Each neuron receives some inputs, performs a dot product and optionally follows it with a non-linearity. The whole network still expresses a single differentiable score function: from the raw image pixels on one end to class scores at the other.

The Pooling Layer

Sometimes when the images are too large, we would need to reduce the number of trainable parameters. It is then desired to periodically introduce pooling layers between subsequent convolution layers. Pooling is done for the sole purpose of reducing the spatial size of the image. Pooling is done independently on each depth dimension; therefore the depth of the image remains unchanged. The most common form of pooling layer generally applied is the max pooling. It is placed in this model to store the secret image finally before starting the network transmission.

Encryption Decryption process

Encryption is defined as the cryptographic technique where the original plain text is converted into cipher text. In this proposed system the image formats that are derived is added with secrecy bits which is transmitted in a secured way, similarly at the receiving end. The end user using the decryption proven, decipher the text to receive the original image.

The Output layer

After multiple layers of convolution and padding, we would need the output in the form of a class. The convolution and pooling layers would only be able to extract features and reduce the number of parameters from the original images. However, to generate the final output we need to apply a fully connected layer to generate an output equal to the number of classes we need. It becomes tough to reach that number with just the convolution layers. Convolution layers generate 3D activation maps while we just need the output as whether or not an image belongs to a particular class. The output layer has a loss function like categorical cross-entropy, to compute the error in prediction. Once the forward pass is complete the back propagation begins to update the error and loss reduction.

7. CONCLUSION

Time series classification is one of the finest input technique to process a network application with respect to the time bound data manipulations executions. To enhance the application of time series classification with respect to the image size, the existing data set classification in the convolutional network are updated with cryptography schemes. This methods also developed to add a crown in the info security domain by providing secret bits in the packets stored in the mechanism. Finally the original data set with respect to security policies are determined early in order to result in 5% increase in process execution.

REFERENCES

[1] Sak, Hasim; Senior, Andrew; Beaufays, Francoise (2014). "Long Short-Term Memory recurrent neural network architectures for large scale acoustic modeling" (PDF).

[2] Felix A. Gers et al (2002) “Learning Precise Timimg with Long Shoet Term Memory Recurrent Networks”

[3] Huiting Zheng et al “ Short-Term Load Forecasting Using EMD-LSTM Neural Networks with a Xgboost Algorithm for Feature Importance Evaluation. - 2017

[4] Ben Athiwaratkun et al – “ Speech and Signal Processing “ (ICASSP)’ – IEEE – 2017.

[5] Zhou. R, Hwang. K, and Cai. M, "Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Network", IEEE - 2018

[6] Abdul-Rahman. A and Hailes.S, "Supporting Trust in Virtual Communities", Conf. System Sciences (HICSS) – 2018

[7] Trupti Katte et al – " Recurrent Neural Network and its various Architecture types – [2018]

[8] Bram Bakker. "Reinforcement learning with Long Short Term Memory "," Advances in neural information processing systems " - Dept. of Psychology, Leiden University, 2002.

[9] Mihir Mongia " Skip Connections and Multiple Matrices in Recurrent Neural Networks " (PDF).

[10] Jeyakumar Kannan, A.R Mohamed Shanavas, and Sridhar Swaminathan, "TwitterSports: Real Time Detection of Key Events from Sports Tweets," Transaction on Machine Learning and Artificial Intelligence, vol. 5, iss. 6, pp. 36-60, 2017. DOI:10.14738/tmlai.56.3729. ISSN 2054-7390. UK