SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Volume 6 No. 3
ISSN 2054-7390

Classification of Encrypted Texts using Deep Learning

[1]Zeinab Nazemi Absardi, [2]Reza Javidan

[1,2]Department of Computer Engineering and IT, Shiraz University of Technology, Shiraz, Iran;

zeinab.nazemi@gmail.com; reza.javidan@gmail.com

ABSTRACT

The most widely used cryptographic systems can identify cryptographic algorithms and identify encryption keys. Statistical methods and learning a variety of machines have been used to identify cryptographic algorithms, each of which has its own advantages and disadvantages. This paper seeks to provide a method for identifying the algorithm used for encrypted texts in text files. Since the volume of this kind of data is very big and increases at any given moment, then the accuracy is calculated by voting of these classifiers. The process of identifying the encryption algorithm is also known from the encrypted texts as the classification of text. So, three methods of encryption AES, RC5, BLOWFISH have been used to evaluate system performance. A three class's classifier is needed, for this purpose, k-nearest neighbor's algorithm has been used. This article is based on a deep learning approach, provides a new method for identifying the pattern in cryptographic texts and learning them by methods of representing features. The proposed method, consists of four parts of the preprocessing, feature learning, data classification and voting. The proposed system's efficiency in algorithm classification is 99.1%.

Keywords: Text classification; Encrypted texts; Deep learning; Encryption algorithms.

1 Introduction

Due to the growing popularity and increased interaction of social media users through conversational texts, the clustering of these types of texts has become an important task. In this paper, a method for clustering texts through deep learning is proposed.

The most widely used cryptographic systems can identify cryptographic algorithms and identify encryption keys. Statistical and machine learning methods have been used to identify the cryptographic algorithm, each of which has its own advantages and disadvantages. Machine learning is a general-purpose method that can learn relationships from the data without the need to define them a priori [1]. For decades, constructing a machine learning system required careful engineering and domain expertise to transform the raw data into a suitable internal representation from which the learning subsystem, often a classifier, could detect patterns in the data set. Conventional techniques are composed of a single, often linear, transformation of the input space and are limited in their ability to process natural data in their raw form [2]. Deep learning allows computational models that are composed of multiple processing layers based on neural networks to learn representations of data with multiple levels of abstraction [3].

The key aspect of deep learning is that these layers of features are not designed by human engineers, but they are learned from data using a general purpose learning procedure. By using a recently proposed leveled homomorphic encryption scheme, it is possible to delegate the execution of a machine learning algorithm to a computing service while retaining confidentiality of the training and test data. Since the

DOI: 10.14738/tmlai.63.4745
Publication Date: 26th June, 2018
URL: http://dx.doi.org/10.14738/tmlai.63.4745

computational complexity of the homomorphic encryption scheme depends primarily on the number of levels of multiplications to be carried out on the encrypted data, we define a new class of machine learning algorithms in which the algorithm's predictions, viewed as functions of the input data, can be expressed as polynomials of bounded degree [4].

There have been numerous studies on classification of encrypted texts which have led to many different approaches. Most of these approaches use predefined features extracted by an expert in order to classify encrypted texts. In contrast, in this study, a deep learning based approach is proposed which integrates both feature extraction and classification phases into one system.

This article seeks to provide a new way of identifying patterns in cryptographic texts and learning them by way of representing features. The system designed for the three encryption algorithms named AES, RC5 and BLOWFISH has been evaluated. It can also be used for other cryptographic algorithms. Section 2 gives a brief overview of the literature in this area. The third Section deals with the proposed methodology and examines the architecture of the system. The tests carried out and the results obtained are also discussed in section four. Finally, Section Five is dedicated to providing conclusions.

2 Review of related works

Classification of encrypted texts has become significantly important with rapid growth of current Internet network and online applications. There have been numerous studies on this topic which have led to many different approaches. In the area of identifying the text encryption algorithm, there are several sections in which the difference in how they implement them has caused differences in the work of various researchers, one of these sections is the choice of how to input the system. Given that the classification of codes based on texts is encrypted. The researchers have used various methods for converting texts into acceptable inputs for the system [5], including the vectorization of strings from texts.

Also, the playback of feature selection and classification is also one of the most influential parts in the design of the classification system of the cryptographic algorithm that results in different results from the performance of the system in different work [6].

One of the most popular classifiers in this area is Naive Bayesian, Support Vector Machine, Neural Network, and Instance Based Leamer. The Naive Bayesian classification is one of the heaviest Bayesian classifiers in terms of calculation, but it has two points compared to others, which is the first to be easy to build. Second, the classification process is very efficient [7].

Also, in the area of detecting the encryption algorithm used in the texts, SVM classifier have been used extensively [8].

Neural network classifiers are also very popular in a variety of domains. In the area of detecting encrypted texts, systems based on the classification of the neural network have shown excellent results that add to the acceptability of this type of classification [9-11].

Network traffic classification has become significantly important with rapid growth of current Internet network and online applications. There have been numerous studies on this topic which have led to many different approaches. Most of these approaches use predefined features extracted by an expert in order to classify network traffic [12].

In [14] a new technique developed to provide solutions for running deep neural networks over encrypted data. They develop new techniques to adopt deep neural networks within the practical limitation of current homomorphic encryption schemes. Test results validate the soundness of approach with several convolutional neural networks with varying number of layers and structures. When applied to the MNIST optical character recognition tasks, this approach achieves 99.52% accuracy which significantly outperforms the state-of-the-art solutions and is very close to the accuracy of the best non-private version, 99.77%. The approach also applied to CIFAR-10, which is much more complex compared to MNIST, and were able to achieve 91.5\% accuracy with approximation polynomials used as activation functions. These results show that CryptoDL provides efficient, accurate and scalable privacy-preserving predictions.

In [13] a novel scheme for a classifier owner is proposed to delegate a remote server to provide the privacy-preserving classification service for users. In the proposed scheme, efficient classification protocols for two concrete classifiers respectively are designed. The prototype of the scheme and conduct tests is implemented. The test results show that the scheme is practical.

3 Proposed Method

One of the most important steps in designing classification systems and clustering information is to select a suitable method for extracting and representing features in the raw input data. The introduction of a learning-based approach to non-monitoring features improves system performance and automatically learns the features of input data. The proposed method consists of four parts of the preprocessing, learning features (representing feature and information retrieval based on the characteristics learned), classification of represented data, and voting. The architecture of proposed system is shown in Figure 1**.**

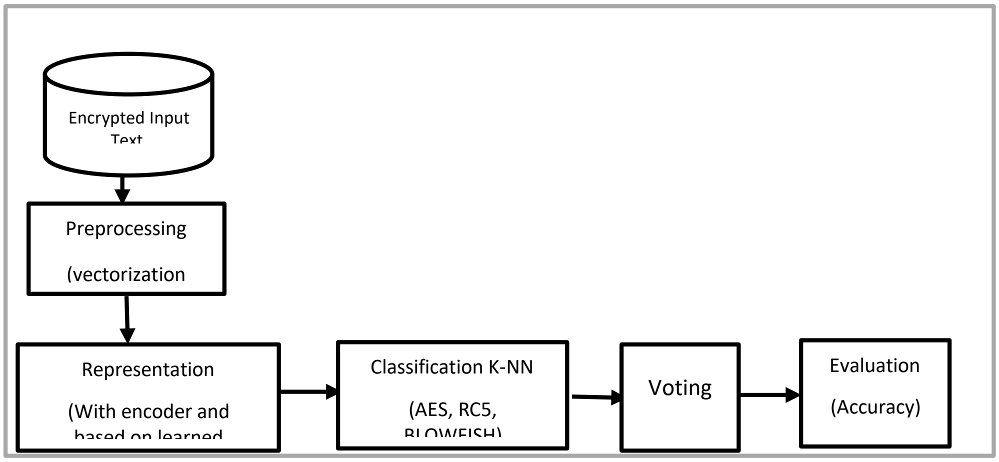

Figure 1. Architecture of proposed method.

3.1 Preprocessing

The preprocessing must first deepen the encrypted text files to match the acceptable input for the neural networks. For this purpose, text vectoring is used. The data used for this study includes three encryption algorithms called AES, RC5 and BLOWFISH, initially similar to the bag of word method in the processing of texts, 500000 strings of 128 bits of the texts of each algorithm are selected. Then put the inputs together and create a collection of 1,500,000 encrypted text strings. The proposed system has two main stages of training and application. At the training stage, the system uses learning resources to learn the best features available in the database. The architecture of the proposed system in the training phase is shown in Figure 2.

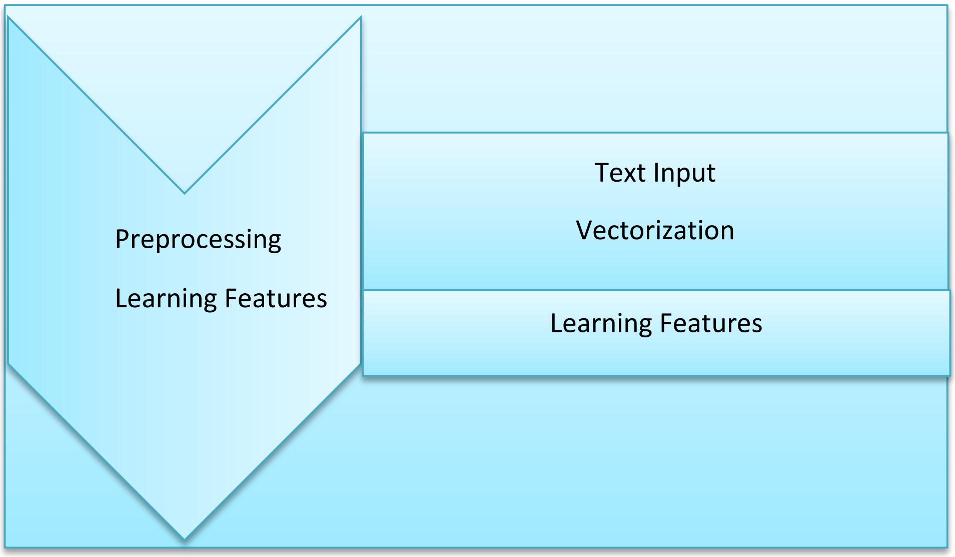

Figure 2. Architecture of the training step.

After learning the features by the cryptography itself, the system is ready to use. In fact, after training, the encoder in the training stage of the system should be able to represent raw data in a new space based on the features learned.

3.2 Learning Features

Learning features are the methods used to representing raw data in the form of a new representational model in the new space. Depending on the issue, this new space can be smaller or larger than the original space. To learn features, a shorter linear encoder has been used shown in Figure 3.

This encoder acts on the basis of a gradient reduction, aiming to create a thumbnail representation of the data. The objective function defined for the predecessor and its related definitions is expressed in Formula 1.

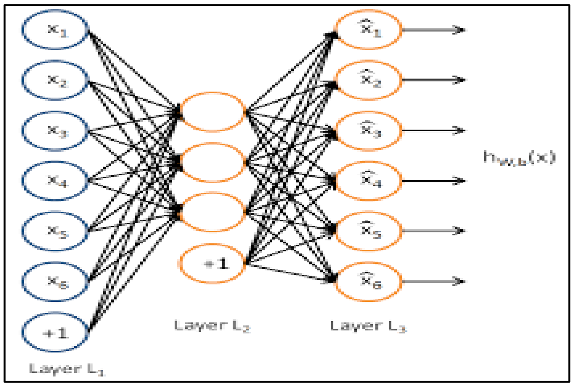

Figure 3. Architecture of encoder in middle layer.

This encoder acts on the basis of a gradient reduction, aiming to create a thumbnail representation of the data. The objective function defined for the predecessor and its related definitions is expressed in Formula 1.

$$Jspace(W,b) = J(W,b) + \beta \sum_{j=1}^{S^s} KL(p \square p$$

$$KL(p \square \widehat{p}j) = p \log \frac{a}{\widehat{p}j} + (1-p)\log \frac{1-a}{1-\widehat{p}j} \qquad (1)$$

$$J(W,b) = \left[\frac{1}{m} \sum_{i-1}^{m} (W,b;x^{(i)},y^{(i)} \right] + \qquad \frac{\lambda}{2} \sum_{j=1}^{nj-i} \sum_{i=1}^{n} \sum_{j=1}^{n+1} (W_{ji}^{(i)})^2$$

In fact, encoder after training on instructional data, the encoder itself becomes a tool to unravel the raw data in an appropriate space for classification. In other words, encoders are a good alternative to traditional method of feature extraction. Especially in cases such as the cryptographic field where the type and gender of the input data are ambiguous, encoders themselves have a high ability. To implement the proposed system based on deep learning, the encoder itself in Figure 3 is designed in three layers, which includes a coding layer, an intermediate layer, and a decoding layer. The given data in accordance with the preprocessing referred to above has become an acceptable input for the system and is sent to the encoder itself with the architecture shown in Figure 4 to be trained with the activation function RELU and the number of replicates of the network is 100,000.

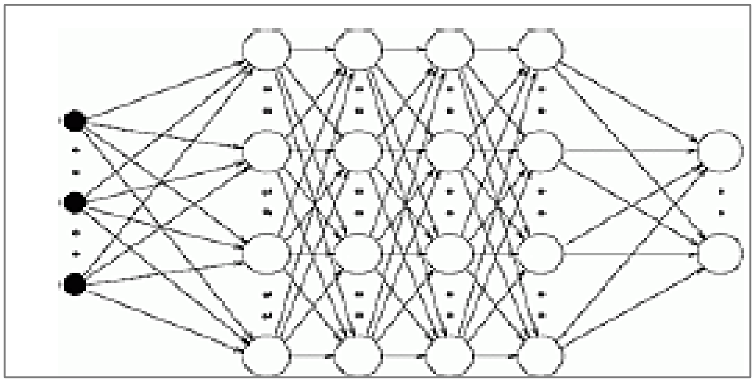

Figure 4. Proposed neural network architecture.

Tag = 3

Decoding layer = 128-256

Intermediate layer = 512

Encoder layer = 128

After learning this encoder, it can be used to represent the raw data in the new space.

3.3 Classification

After representing raw inputs, it is time to classify them. In this system, this study is trying to identify the method of encryption of input data. As mentioned above, in this research, RC5 AES and BLOWFISH encryption methods have been used to evaluate system performance. So in this system a class of three classes is needed. For this purpose, a KNN classifier has been used based on the Mahalanobis distance. Because of its high codec capability in representing raw data, a simple classifier of KNNs has the ability to properly handle data. Also, due to the lack of need for this class of classifier, learning and training, if the number of classifier is changed (changing the number of cryptographic algorithms), this classifier of categories easily adapts itself.

3.4 Voting

As stated, the encoder represents the extracted vectors from raw input data using the learned features. After representing these vectors, they classify their categories and determine which algorithms are encrypted. But the purpose of this system is to detect the encryption algorithm of a text. According to the description given, a text contains much number of words that are made in the form of a vector in this system. As a result, to decide on a text, one can extract the results of multiple vector classifications and decide on the results of their classification. This final decision is taken by a majority vote.

4 Evaluation of Proposed Method

To evaluate the proposed system, 128-bit characters are randomly generated to be used in the training and testing of the system. Also, to test the system more precisely, two test models were performed on this system. In the first approach, despite the difference in the training and testing data classification, the key to their encryption is the same. In the second method, the cryptographic key of the training data is completely different with the test data. It is important to note that in all of the above methods, the encryption key for the encoder's own learning resources, which is used to extract the property; it is different from other educational and test tutorials in the upper hand. To evaluate the proposed system, 500000 vectors of 128 selected from each algorithm are put together to create a collection of 1,500,000 vectors of encrypted texts by the three algorithms.

a KNN classifier based on k = 10 was used for evaluating the proposed architecture of encoder that the percentage of system performance in the same way as the cryptographic key of the training and test data of the cluster was 84.3%, and in the case of different cryptographic keys, the training and test data of the cluster was 39.9%. Given that at the time of the test, in real terms, every text file received a large number of test inputs. Finally, the final view of the system for that text file is presented, a test was presented based on this. In this test, for each text file, 100 samples of 128 bits are tested, then, by voting in the votes obtained from the system for 100 samples, the final commentary on the input text file is presented. According to the conditions mentioned above, the system performance was equal to 99.1 percent for the same key and 62.5 percent for the encryption key. In Table 1 and 2, the efficiency of the system has been investigated.

Table 1. Accuracy of classification of encoded vectors.

Algorithm Key	Accuracy of Classification
same for train and test data	84.3
different for train and test data	39.9

Table 2. Accuracy of classification of encoded vectors voting.

Algorithm Key	Accuracy of Classification
same for train and test data	99.1
different for train and test data	62.5

Considering the different conditions of training and testing in the systematic analysis systems, in these studies, there is generally no comparison with past work to implement the proposed system, the CAFFE profound learning framework has been used. Testing and analyzing outcomes have also been done in MATLAB software.

5 Conclusion

In this article a new method for classifying encrypted texts is presented. In this way, a deep network was provided to receive input data from various algorithms and to train their features and eventually represent them in a suitable environment. This paper seeks to provide a method for identifying the algorithm used for encrypted texts in text files. Since the volume of this kind of data is very big and increases at any given moment, then the accuracy is calculated by voting of these classifiers. So, three methods of encryption AES, RC5, BLOWFISH have been used to evaluate system performance. Also there are several methods for classifying cryptographic algorithms. In this system a three class's classifier is needed. For this purpose, k-nearest neighbor's algorithm (K-NN) has been used. This article is looking for a deep learning-based approach. In order to analyze the input data, the proposed method consists of four parts of the preprocessing, feature learning, data classification and voting. This paper, seeks to provide a new method for identifying the pattern in cryptographic texts and learning them by methods of representing features. The system designed for the three encryption algorithms named BLOWFISH, RC5, and AES is evaluated and can be generalized for use with other cryptographic algorithms. The proposed system's efficiency in algorithm classification is 98.9%. Subsequently, by the same network trained, the data was represented in a new space and classified by the KNN category and the maximum voting method. Given that this method has been tested for a limited number of cryptographic algorithms, it can be evaluated for a range of algorithms and, if possible, create similar conditions, the results will be compared with other similar work carried out in this area. There are also various parameters in the deep design grid that can be modified and reviewed by their results to optimize the system.

REFERENCES

[1] Murphy Kevin P. *Machine learning: a probabilistic perspective*, MIT press, 2012. p. 119-121.

[2] Bengio Y. et al, *Representation learning: a review and new perspectives*. IEEE Trans Pattern Anal Mach Intell, 2013. 35(4): p. 1798–828,.

[3] LeCun Y. et al, *Deep learning*, Nature, 2015. p. 436–44.

[4] Graepel T. et al , *ML Confidential: Machine Learning on Encrypted Data*. Information Security and Cryptology ICISC, 2012.

[5] Liwen Peng and Yongguo Liu, *Feature Selection and Overlapping Clustering-Based Multilabel Classification Model*, Mathematical Problems in Engineering, vol. 2018, 281489.

[6] H. Peng, F. Long, and C. Ding, *Feature selection based on mutual information: criteria of max-dependency, max-relevance, and min-redundancy*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2005. 27(8):p. 1226–1238.

[7] J. Nayak, et. al, *Fuzzy C-means (FCM) clustering algorithm: a decade review from 2000 to 2014 in Computational Intelligence in Data Mining*—Volume 2, L. C. Jain, H. S. Behera, J. K. Mandal, and D. P. Mohapatra, Eds., vol. 32 of Smart Innovation, Systems and Technologies, Springer, 2015. p. 133–149.

[8] D. Mena. et al, *An overview of inference methods in probabilistic classifier chains for multilabel classification*, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2016. 36(6):p. 215–230.

[9] F. Chamroukhi, D. Nguyen, *Model-Based Clustering and Classification of Functional Data*, 2018, arXiv: 1803.00276[cs.CR] .

[10] Xiaohong, G., et al. *A method of vessel tracking for vessel diameter measurement on retinal images*. in Image Processing. Proceedings. International Conference on, 2001.

[11] J. Lee and D. W. Kim, *Memetic feature selection algorithm for multi-label classification*, *Information Sciences*, 2015. 293(3):p. 80–96.

[12] M. Lotfollahi. et al , *Deep Packet: A Novel Approach For Encrypted Traffic Classification Using Deep Learning*, 2017. arXiv:1709.02656 [cs.LG].

[13] T. Li, et al. *Outsourced privacy-preserving classification service over encrypted data*, Journal of Network and Computer Applications,2018. p. 100-110.

[14] Ehsan Hesamifard. et al, *CryptoDL: Deep Neural Networks over Encrypted Data*, arXiv:1711.05189 [cs.CR], 2017. p. 347-364,.