Encryption scheme classification : a deep learning approach

Pan, Jonathan

2017

Pan, J. (2017). Encryption scheme classification: a deep learning approach. International Journal of Electronic Security and Digital Forensics, 9(4), 381-395.
doi:10.1504/IJESDF.2017.087397

<https://hdl.handle.net/10356/144715>

<https://doi.org/10.1504/IJESDF.2017.087397>

© 2017 Inderscience. All rights reserved. This paper was published in International Journal of Electronic Security and Digital Forensics and is made available with permission of Inderscience.

Downloaded on 26 Apr 2023 08:54:04 SGT

Encryption Scheme Classification : A Deep Learning Approach

Jonathan Pan*

Wee Kim Wee School of Communication and Information

Nanyang Technological University

Singapore

E-mail: jonathan.pan.jy@gmail.com

*Corresponding author

Abstract— Encryption has an important role in protecting cyber assets. However use of weak encryption algorithms could render this intent useless as it could be exploited to gain unauthorized access to these important assets. This vulnerability may be exploited intentionally. Hence this vulnerability has been formally recognized with its own Common Vulnerabilities and Exposures (CVE) label by cyber security community as the vulnerability to protect. When exploited, detecting this vulnerability from encrypted data is very difficult task to undertake. This research explores the use of recent advancement in machine learning algorithms specifically deep learning algorithms to classify encryption schemes based on entropy measurements of encrypted data with no feature engineering. Past research work using various machine learning algorithms have failed to achieve good accuracy results in classification. The research entails applying encryption algorithms Data Encryption Standard (DES) and Advanced Encryption Standard (AES) with block cipher modes namely Electronic Codebook (ECB) and Cipher Block Chaining (CBC) over the image dataset from CIFAR10. Two ImageNet winning Convolutional Neural Network deep learning models namely AlexNet and GoogleNet are used to perform the classification. Transfer learning and layer modification were applied to evaluate the classification effectiveness. This research concludes that deep learning algorithms can be used to perform such classification where other algorithms have failed.

Index Terms— Encryption Classification, Deep Learning, Artificial Intelligence

Biographical Notes: Jonathan Pan is currently a Part-Time Lecturer at the Wee Kim Wee School of Communication and Information, Nanyang Technological University, Singapore. He received his doctoral degree in Information Technology from Murdoch University and Master of Technology Management from University of Queensland and Bachelor of Computer Science from University of Newcastle, Australia. His research interests are in Cyber Security and Artificial Intelligence. He authored over 10 papers in journals and proceedings of international conferences.

1 Introduction

Information security is about protecting Information Technology assets like data, computing resources and e-transactions through the upkeep of their confidentiality, integrity and availability. A commonly used technical approach to achieve such information security desired objectives is through the application of encryption. Encryption involves the use of special mathematical algorithms to convert discernable data in its plain or readable form by software or by humans also known as plaintext to a form that is unreadable or non-interpretable form also known as ciphertext. The encrypted data or ciphertext is only readable after a matching decryption process converts the unreadable form back to its original readable form. Generally, valid decryption entails the use of the matching decryption algorithm to the encryption algorithm with the needed decryption key.

Encryption is applied to data stored in a various storage mediums and when data is transported from one location to another. Encryption can be applied to the varied data formats from textual data to video, audio and images.

While encryption of data is intended to protect the data from Information Security breaches, poor application of weak encryption algorithms will render the intent useless. Through the application of Cryptanalysis procedures like the Cryptographic Distinguishing Analysis of identifying the applied encryption algorithm, encrypted data could be deciphered through matching of decryption algorithm and subsequent search for the valid decryption key. The latter (search of valid key) may be determined through brute force or forms of heuristic determination.

Such vulnerabilities have been intentionally exploited by hackers or Malware or unintentionally applied by misconfiguration of the choice of encryption algorithm.

In order to detect the exploitation of such vulnerability within encrypted data that is not easily distinguishable by humans or machines, there are past research work to explore the use of machine learning algorithms to classify encryption scheme used based on samplings of encrypted data. However according to Chou et al. (Chou et al., 2012), there has been limited successes in developing suitable machine learning models to effectively perform cryptanalysis. However in recent years, there has been a significant development in deep learning algorithms that greatly enhance the classification capabilities of machine learning algorithms. The intent of this research work is to assess whether contemporary deep learning algorithms specifically with Convolution Neural Networks (CNN) may be used to classify encryption schemes over encrypted images without any feature engineering done. In order to test this hypothesis, two winning CNN models that have different model architecture but each having won the ImageNet (Deng et al., 2009) competition were trained for the task. Additionally recently development in deep learning algorithms highlighted the effectiveness of using deeper models (Szegedy et al., 2014), (Simonyan and Zisserman, 2014), (Wang et al., 2015), hence the second hypothesis of this research is to assess the effects of the depth of CNN in encryption scheme classification.

In the next section of this paper, the background about the risk of weak encryption and brief introduction to the deep learning algorithm used in this research will be covered. This is followed by a review of related research, then by a description of the experiments conducted for this research. An analysis of the experiment follows. Finally, a conclusion and discussion on the future research direction.

2 Background

The following details the vulnerability of using weak encryption and a brief introduction to Convolutional Neural Network deep learning algorithm specifically two such models with differing architecture structures used in this research.

2.1 Encryption

Encryption is done through the application of mathematical based cryptographic algorithms that turns clear text to encrypted form. The following equation illustrates simply how generally cryptographic algorithms convert plaintext to ciphertext and back from ciphertext to plaintext.

$$C = E(P, K_E) \quad (1)$$

$$P = D(C, K_D) \quad (2)$$

P represents plaintext or readable data, C represents ciphertext or encrypted data, K_E and K_D represent the keys used to perform the encryption and decryption process respectively. Depending of the type of encryption / decryption scheme or algorithm used, both keys may be the same. E and D functions represent the encryption and decryption process. These functions are matched to achieve the intended outcome of converting plaintext to ciphertext and back. Hence identification or knowledge of the encryption scheme used is a vital step towards eventual decryption.

Each encryption algorithm has its own set of cryptographic characteristics in terms of its ability to protect its contents from attempts to reverse the encryption or to distinguish characteristics of the applied cryptography. According to Jorstad from National Institute of Standards and Technology (Jorstad, 1997)**Error! Reference source not found.**, discovery of cryptographic algorithm or the encryption scheme applied would substantially reduce the resources required to break the cryptosystem.

An analysis done by Arora (Arora, 2012) assessed that Data Encryption Standard (DES), once a dominant encryption algorithm, to be a relatively weak encryption algorithm. It supports 56 bits of password. The number of possible combinations of passwords for 56 bits is 7.2×10^{16} .

Many attempts have been made to break this encryption. Eventually in Jan 1999, it was broken in 22 hours and 15 minutes. With the advancement of computing capabilities, DES encrypted data can be quickly broken. A relatively stronger encryption algorithm is the Advanced Encryption Standard (AES) whose password length extends to 256 bits which has 1.1×10^{77} possible combinations. Using a Fast Supercomputer with 10.51 Petaflops, the DES 56 bit encryption will take 399 seconds to crack. The AES 256-bit encryption will take 3.31×10^{56} years to crack.

Hence weak encryption would render the encryption near useless when exposed to a strong Cryptoanalysis procedure. The Cryptoanalysis procedure is the technical analysis of ciphertext or encrypted data to forensically attempt to reverse the applied encryption to achieve the desired objective of retrieving the original plaintext or data in its original non-encrypted form. One phase of the Cryptoanalysis is the Cryptographic Distinguishing Analysis involving the extraction of samplings of the encrypted message and attempting to identify the encryption algorithm used to produce the encrypted messages. Once the encryption algorithm or encryption scheme has been identified, the Cryptoanalysis' objective is partially achieved with the password as the remaining piece to the puzzle. This may be done with brute force or forms of heuristic approaches. This research will focus on the identification of the encryption scheme used less in the determination of the passphrase used.

2.2 Effects of Weak Encryption

The primary risk associated with the use of weak encryption is the inability to maintain confidentiality of data to which encryption was intended to upkeep. With weak encryption, the encrypted data can be mistaken to be securely protected though it can be easily be decrypted under unauthorized or undesirable actors.

A misconfiguration in software that uses weak encryption algorithm would incentivize hackers to steal the encrypted data and attempt to break the weak encryption to recover the data in its original form. Conversely a strong encryption would dis-incentivize the hacker as any attempt to break a strong encryption could result in wasted pro-longed periods of attempts. The Common Vulnerability Enumeration listing from MITRE (CVE, 2003)⁰ for such vulnerability is the CVE 326 that is defined as "Inadequate Encryption Strength" where the encryption scheme used that is theoretically sound but is not strong for level of the protection required. According to Howard et al. (Howard et al., 2010) who wrote the book on "24 Deadly Sins of Software Security", the use of wrong cryptography is deemed a sin.

2.3 Deep Learning Algorithms

The deep learning algorithms is a branch of machine learning algorithms that produces high level abstraction of data through multiple neural network layers and non-linear transformations. A popular deep learning classification algorithm is the Convolution Neural Network (CNN) that has recently achieved significant success in classifying images, sound and video with very high degree of accuracy. This form of feed forward neural network architecture is inspired by the structure of the visual cortex (Lawrence, 1997). This entails the use of multiple overlapping tiles of visual field receptors or known as filters to process inputs to identify common features. The combination of the convolutional layers provides the means to group granular features to identify more abstract features. Various forms of regularization techniques may be used like dropout and max-pooling.

There is a number key characteristics of the CNN architecture. One is its ability to identify spatially local correlations in the input data. Another is the network's invariance to translations, rotations or scaling. Finally is its ability to perform unsupervised feature detection with little to no feature engineering effort required as compared to other conventional forms of machine learning algorithms.

3 Related Work

Chopra and Satav (Chopra and Satav, 2013) evaluated the performance of Naïve Bayesian and K-Nearest neighbour algorithms to classify encrypted dataset. Various performance measurement techniques were used to assess classification namely accuracy, precision and

recall. The decision tree C5.0 algorithm performed best with a wide variation of accuracy ranging from 60% to 99% with fare amount of feature engineering involved.

Sharif and Mansoor (Sharif and Mansoor, 2011) used eight commonly used machine learning classification algorithms, namely Naïve Bayesian (NB), Support Vector Machine (SVM), neural network (MLP), Instance based learning (IBL), Bagging (Ba), AdaBoostM1 (MdaBM1), Rotation Forest (RoFo), and Decision Tree (C4. 5), to perform cryptanalysis on ciphertext based on the 8 bit histogram of the encrypted text as the feature sets. Four popular encryption algorithms namely AES, Rivest Cipher (RC2), DES and International Data Encryption Algorithm (IDEA) operating in Electronic Cookbook (ECB) mode were. Their result showed that using pattern recognition may be used to identify the encryption algorithm when their simulation used one encryption of key in comparison to using different keys. Additionally, when the number of the encrypted input files to train the algorithms, these algorithms improved in their accuracy measurements. Their research however showed that accuracy scores ranges from 40% onwards which again has a large variation of accuracy.

The research work by Chou et al. (Chou et al., 2012) challenged previous research work in the use of machine learning classification algorithms to classify encryption scheme. They did so by applying state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks on several public datasets including text, images and audio files on the commonly used encryption schemes of DES and AES using different modes of operation. They found that when Cipher Block Chaining (CBC) mode is used with a random initial vector for each plaintext, the performance is extremely bad, while the performance for certain datasets is relatively good when ECB mode is used.

Chou et. al also reviewed that the work by Manjula and Anitha (Manjula and Anitha, 2011) that proposed the use of several features namely the entropy measurement and correlation coefficient of certain classes of data types and size of files to identify the encryption algorithms using decision tree. Chou et. al concluded that their approach to use decision tree algorithm could only classify correctly to about 50% of the time that implies that this is as effective as tossing of coin.

Hence past attempts in using machine learning algorithms to perform encryption scheme classification with entropy measurement have not yielded accepted performance outcomes due to the large variation in accuracy measurements.

4 Method

The research experiment started with the preparation of encrypted data needed to train, cross-validate and test the Convolutional Neural Network models. There was also the model preparation step to prepare the models through transfer learning from pre-trained models to accelerate model training. The second hypothesis test required model modification to the base AlexNet and GoogleNet models. Finally a set of accuracy measurements was used to assess the models.

4.1 Data Preparation

The base dataset used to produce the model for encryption scheme classification consists of a set of images. They are a subset of the CIFAR10 image dataset that is a labeled subset of the 80 million tiny images (Torrvalba et al., 2008). The base dataset will compromise of six out of the ten CIFAR10 image categories. The base dataset was further divided into two subsets. One subset of four image categories was used for training and validation of the deep learning models. They are the 'automobile', 'cat', 'dog' and 'truck' categories. Another subset of one image category was used for testing the model. That image category was the 'airplane' category. Each category of images numbered to 5,000.

With the base dataset, the following encryption schemes were applied.

- DES-ECB with 56 bit encryption key
- DES-CBC with 56 bit encryption key
- AES-ECB with 256 bit encryption key
- AES-CBC with 256 bit encryption key

Hence the total number of images produced for training and cross validation for the four encryption schemes numbers 80,000 and 20,000 for testing. The training and cross-validation dataset were further divided into 90% for training and 10% for cross-validation.

The open source OpenSSL (OpenSSL) tool running on Ubuntu was used to perform the encryption against the four classes of encryption schemes. The choice and length of password used were constant to facilitate the design of this experiment.

4.2 Model Preparation

The Convolution Neural Network (CNN) deep learning algorithm was used in this research. Instead of constructing a brand new Convolution Neural Network from scratch, this research reused existing CNN models that have demonstrated its ability to classify complex images through the ImageNet competition. The CNN base models used will be the AlexNet model (Krizhevsky et al., 2012) and the GoogleNet model (Szegedy et al., 2014). Both models had won past ImageNet competitions in year 2012 and 2014 respectively. AlexNet has 5 convolutional layers capped with three fully connected neural network layers with softmax to the output layers. The model has 60 million hyperparameters. The following diagram depicts this model architecture.

Fig. 1. AlexNet's Architecture

The GoogleNet model uses a different architecture codenamed "Inception" that approximates sparse structure with spatially repeated dense components and adopts dimensionality reduction to maintain computational complexities. This has resulted in fewer hyperparameters as compared to AlexNet (about 5 million). There is however 22 layers embedded with 9 "Inception" modules. The key benefits of this architectural model are to maintain computational complexities regardless of processing units and faster performance as compared to other architectures. The following diagram depicts the "Inception" module used in GoogleNet.

Fig. 2. GoogleNet's Architecture

There are the common model parameters that one can manipulate when applying CNN to classification problems. This includes the filter size, type of pooling, number of filters, stride dimensions and zero padding configuration of the model. Additionally, the learning rate could be altered during the training stage to optimize model development. These were left unchanged as part of the design of this experiment. However as one of the research hypothesis is to study the effects of depth of deep learning algorithms on this classification problem, the depth of the models were varied or more specifically increased to test the effectiveness of deeper models. According to He and Sun (He and Sun, 2015), the most important CNN feature is having deep architecture. Other recent research works (Szegedy et al., 2014), (Simonyan and Zisserman, 2014), (Wang et al., 2015) indicate that the deeper the layers, the more capable are the algorithms in picking up subtle patterns in encrypted data. Along this line, the two base model architectures (AlexNet and GoogleNet) were modified to test this hypothesis. The following illustrates the modification done with AlexNet to include an additional Convolutional Layer labeled "*Conv LayerN*".

Fig. 3. Modified AlexNet with One Additional Convolutional Layer

With the base models and modifications made to increase the layers, the following were the models used in this research.

- Standard AlexNet
- AlexNet with one additional layer
- AlexNet with two additional layers
- Standard GoogleNet
- GoogleNet with one additional layer
- GoogleNet with two additional layers

Before the models were training and assessed, another model preparation step was taken. There has been much research literature highlighting the benefits of using transfer learning that involves training a model first with a comprehensive dataset for classification and performing re-training on the trained model with actual dataset to quicken the training process (Oquab et al., 2014), (Ciresan et al., 2012). Hence pre-training was done on both AlexNet and

GoogleNet base models using non-encrypted CIFAR10 image data. The resultant pre-trained models are then trained with encrypted images from the prepared training and cross-validation dataset.

The subsequent training and cross-validation of the models was done using Caffe (Jia, 2013) with NVIDIA's DIGITS (<https://developer.nvidia.com/digits>) with dual GPUs.

Fig. 4. Training Results from NVIDIA's DIGITS

The training of each model took 30 epochs. The reason for the short training cycle was primarily because of the limits research resources available and prolonged time needed to carry out the training. However the following training visualization group shows that the training epochs is sufficient as the validation loss and accuracy reaches saturation by the midway through the training stage. Due to the pre-training model preparation and transfer learning steps taken earlier, the model responded quickly to the new training dataset.

4.3 Evaluation

The evaluation or testing of the trained models was done with the testing dataset that used the same set of encryption schemes. The evaluation was done with pairs of encryption schemes. The following are the comparative list used in the test.

- ECB vs CBC with DES
- ECB vs CBC with AES
- AES vs DES with ECB
- AES vs DES with CBC

The classification evaluation of the base models was first done on the base CNN models using Confusion Matrix. Following which, all models including the depth modified models were evaluated using the measurements of TP (true positive) for valid classification of selected encryption scheme and FP (false positive) for wrong classification. The Precision, Recall, Accuracy and F1-Score (denoted as F1) measurements were then computed using the following formulas.

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

$$Recall = \frac{TP}{TP + FN} \quad (4)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (5)$$

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (6)$$

This research involved the classification tests of pairs of encryption schemes. This can be easily extended to perform multi-class classification.

5 Analysis

Following the conduct of the experiments, the classification results were analyzed to assess the performance of the trained models. The first set of analysis is to perform classification evaluation of both base models. The next set of analysis is to assess the effects of the modified models with deeper layers. The last set of analysis is a literature survey dealing with the vulnerability of weak encryption specifically when encrypting images.

5.1 Base Models Evaluation

The following is Confusion Matrix assessment results for the base models used in this research.

	Predicted DES-ECB	Predicted DES-CBC
Actual DES-ECB	4651 (GoogleNet), 4685 (AlexNet)	345 (GoogleNet), 311 (AlexNet)
Actual DES-CBC	0 (GoogleNet), 15 (AlexNet)	4998 (GoogleNet), 4983 (AlexNet)

Table 1 – DES-ECB vs DES-CBC

	Predicted AES-256-CBC	Predicted AES-256-ECB
Actual AES-256-CBC	4999 (GoogleNet), 4999 (AlexNet)	0 (GoogleNet), 0 (AlexNet)
Actual AES-256-ECB	1097 (GoogleNet), 1964 (AlexNet)	3903 (GoogleNet), 3036 (AlexNet)

Table 2 – AES-256-CBC vs AES-256-ECB

	Predicted AES-256-ECB	Predicted DES-ECB
Actual AES-256-ECB	4722 (GoogleNet), 4681 (AlexNet)	278 (GoogleNet), 319 (AlexNet)
Actual DES-ECB	1288 (GoogleNet), 2363 (AlexNet)	3708 (GoogleNet), 2633 (AlexNet)

Table 3 – AES-256-ECB vs DES-ECB

Predicted AES-256-CBC	Predicted DES-CBC
--------------------------	----------------------

Actual AES-256-CBC	2389 (GoogleNet), 2547 (AlexNet)	2610 (GoogleNet), 2452 (AlexNet)
Actual DES-CBC	2417 (GoogleNet), 2458 (AlexNet)	2581 (GoogleNet), 2540 (AlexNet)

Table 4 – AES-256-CBC vs DES-CBC

Both GoogleNet and AlexNet models performed well in classifying encrypted images with the exception of CBC block cipher. Also noted that GoogleNet slightly performed better over AlexNet. In comparison with the research done previously on entropy analysis (Chou et al., 2012), (Manjula and Anitha, 2011), the Convolutional Neural Network algorithms performed significantly better in classifying pairs of encryption scheme. The only exception noted was encryption with CBC block cipher scheme. This is a valid outcome as CBC removes local proximity characteristics or embedded patterns from the unencrypted data.

5.2 Deep Layer Evaluation

The following are the results of the experiment measured in Precision, Recall, Accuracy and F1-Score values for the base and modified models.

Classification Test	Model	Precision	Recall	Accuracy	F1-Score
DES-ECB vs DES-CBC	GoogleNet	100.00%	93.09%	96.55%	0.96
DES-ECB vs DES-CBC	GoogleNet + 1	100.00%	93.33%	96.67%	0.97
DES-ECB vs DES-CBC	GoogleNet + 2	100.00%	93.55%	96.78%	0.97
DES-ECB vs DES-CBC	AlexNet	99.68%	93.78%	96.74%	0.97
DES-ECB vs DES-CBC	AlexNet + 1	49.99%	100.00%	49.99%	0.67
DES-ECB vs DES-CBC	AlexNet + 2	49.99%	100.00%	49.99%	0.67
AES-CBC vs AES-ECB	GoogleNet	82.00%	100.00%	89.03%	0.90
AES-CBC vs AES-ECB	GoogleNet + 1	82.02%	100.00%	89.04%	0.90
AES-CBC vs AES-ECB	GoogleNet + 2	100.00%	100.00%	100.00%	1.00
AES-CBC vs AES-ECB	AlexNet	71.79%	100.00%	80.36%	0.84
AES-CBC vs AES-ECB	AlexNet + 1	50.01%	100.00%	50.01%	0.67
AES-CBC vs AES-ECB	AlexNet + 2	96.57%	9.56%	54.62%	0.17
AES-ECB vs DES-ECB	GoogleNet	78.57%	94.44%	84.33%	0.86
AES-ECB vs DES-ECB	GoogleNet + 1	71.75%	93.48%	78.33%	0.81
AES-ECB vs DES-ECB	GoogleNet + 2	72.44%	93.46%	78.94%	0.82
AES-ECB vs DES-ECB	AlexNet	66.45%	93.62%	73.17%	0.78
AES-ECB vs DES-ECB	AlexNet + 1	97.18%	15.88%	57.69%	0.27
AES-ECB vs DES-ECB	AlexNet + 2	95.89%	14.48%	56.91%	0.25
AES-CBC vs DES-CBC	GoogleNet	49.71%	47.79%	49.71%	0.49
AES-CBC vs DES-CBC	GoogleNet + 1	49.84%	91.70%	49.70%	0.65
AES-CBC vs DES-CBC	GoogleNet + 2	50.02%	99.92%	50.04%	0.67
AES-CBC vs DES-CBC	AlexNet	50.89%	50.95%	50.89%	0.51
AES-CBC vs DES-CBC	AlexNet + 1	47.66%	4.08%	49.79%	0.08
AES-CBC vs DES-CBC	AlexNet + 2	50.01%	100.00%	50.01%	0.67

Table 5 – Results From Experiments

There was measure of improvements when there were increased in the depth of the layers to the GoogleNet model. However with the AlexNet model, the increased in depth worsen the classification accuracy. The following charts compare the models' performance for the pairs of encryption scheme comparison.

Figure 5 – DES-ECB vs DES-CBC

Figure 6 – AES-CBC vs AES-ECB

Figure 7 – AES-ECB vs DES-ECB

Figure 8 – AES-CBC vs DES-CBC

5.3 Image Encryption

In this experiment, images were used as the base dataset to evaluate the classification effectiveness of deep learning algorithms. Image, stored in digital form, has high correlational properties with adjacent cells or pixels. Due to this property, the use of weak encryption scheme over images may retain such correlational property even after encryption. Hence an adequately strong classification algorithm would be able to pick up such patterns. However strong encryption algorithms, specifically those that attempt to remove such correlational characteristics like the Cipher Block Chaining (CBC), would address this problem. CBC takes each block of plaintext or unencrypted data and XORed it with the previous ciphertext block before being encrypted. Hence each ciphertext block depends on all plaintext blocks processed up to that point that in turn removes such data correlations. This is validated through this research's experiment as the deep learning algorithms could not accurately classify the encrypted images produced by CBC.

Aside from CBC, John Justin and Manimurugan (John Justin and Manimurugan, 2012) suggested that different chaotic maps can be used. Chaos based algorithm takes the approach of scrambling pixels of image to remove or reduce the correlation among pixels. Kamali et al. (Kamali et al., 2010) proposed an image encryption algorithm that enhances the Advanced Encryption Standard algorithm. The authors proposed modification to the process be done by adjusting the Shift Row Transformation. According to their experiment result, the modified encryption algorithm produces very good encryption results focusing towards the security against statistical attacks.

6 Conclusion & Future Directions

Deep learning algorithms specifically Convolutional Neural Networks could classify encryption schemes to good level of accuracy based on entropic characteristics of the encrypted data. In this research, the winning models from ImageNet (AlexNet and GoogleNet) were used with no feature engineering applied to the dataset for training, cross-validation and testing. The models were further modified to deeper the network architecture of these models. Generally GoogleNet with its Inception modules performed better with deeper network structures as compared to typical Convolutional Neural Network structures.

Future research work could involve variation to primary model parameters of the Convolutional Neural Network like the stride, depth, types of regularization, etc to assess which primary parameters would improve the performance of such models. Also an ensemble of machine learning algorithms coupled with Convolutional Neural Networks could be applied to further improve the accuracy of encryption scheme classification.

References

- Arora M. (2012), How secure is AES against brute force attacks?, EE Times, [Online]. Available: http://www.eetimes.com/document.asp?doc_id=1279619. [Accessed Jul. 29, 2016].
- Chopra J. and Satav S. (2013), Impact of Encryption Techniques on Classification Algorithm for Privacy Preservation of Data, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 10, Oct 2013, pp. 5398-5402.
- Chou J. W., Lin S. D. and Cheng C. M. (2012), On the effectiveness of using state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks, Proceedings of the 5th ACM workshop on Security and artificial intelligence, ACM New York, USA, pp. 105-110.
- Ciresan D. C., Meier U. and Schmidhuber J. (2012), Transfer learning for Latin and Chinese characters with deep neural networks, International Joint Conference on Neural Networks (IJCNN), pp 1301-1306.
- CVE (2003), Common vulnerabilities and exposures", MITRE, [Online]. Available: <http://www.cve.mitre.org/>. [Accessed Jul. 29, 2016]
- Deng J., Dong W., Socher R., Li L.-J., Li K., and Fei-Fei L. (2009), ImageNet: A Large-Scale Hierarchical Image Database, In CVPR09.
- He K. and Sun J.(2015), Convolutional neural networks at constrained time cost. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- Howard M., LeBlanc D. and Viega J.(2010), 24 Deadly Sins of Software Security, pp. 315, McGraw-Hill.
- Jia Y. (2013), Caffe: An open source convolutional architecture for fast feature embedding. [Online]. Available: <http://caffe.berkeleyvision.org/>. [Accessed Jul. 29, 2016].
- John Justin M. and Manimurugan S. (2012), A Survey on Various Encryption Techniques, IJSCE, Volume-2, Issue-1, March 2012, pp. 429-432, ISSN: 2231-2307.
- Jorstad N. D. (1997), "Cryptographic Algorithm Metrics", Institute for Defense Analyses Science and Technology Division.
- Kamali S. H., Shakerian R., Hedayati M. and Rahmani M. (2010), A New Modified Version of Advanced Encryption Standard(AES) Based Algorithm for Image Encryption, IEEE Transactions on Electronics and Information Engineering, Vol 1, pp.141-145.
- Krizhevsky A., Sutskever I. and Hinton G. E. (2012), ImageNet Classification with Deep Convolutional Neural Networks, Advances in Neural Information Processing System 25 (NIPS, 2012), pp 1106-1114.
- Lawrence S., Giles C. L., Tsoi A. C. and Back A. D. (1997), Face recognition: A convolutional neural-network approach, IEEE Trans. Neural Netw. 8, 98-113.
- Manjula R. and Anitha R. (2011), Identification of Encryption Algorithm Using Decision Tree. Advanced Computing Communications in Computer and Information Science 2011 Volume 133, Part 3, 237-246.
- Oquab M., Bottou L., Laptev I., and Sivic J. (2014), Learning and Transferring Mid-Level Image Representations using Convolutional Neural Networks, In Proc. CVPR.

OpenSSL, The OpenSSL project. OpenSSL—cryptography and SSL/TLS toolkit. [Online]. Available: <http://www.openssl.org>. [Accessed Jul. 29, 2016].

Sharif S. O. and Mansoor S. P. (2011), Performance Evaluation of Classifiers used for Identification of Encryption Algorithms, Proceedings of International Conference on Advances in Information and Communication Technologies.

Simonyan K. and Zisserman A. (2014), Very deep convolutional networks for large-scale image recognition, arXiv preprint arXiv:1409.1556.

Szegedy C., Liu W., Jia Y., Sermanet P., Reed S., Anguelov D., Erhan D., Vanhoucke V., and Rabinovich A. (2014), "Going deeper with convolutions" CoRR, abs/1409.4842.

Torralba A., Fergus R., and Freeman W. (2008), 80 million tiny images: A large data set for nonparametric object and scene recognition. IEEE PAMI, 30(11):1958–1970.

Wang L., Lee C., Tu Z., and Lazebnik S. (2015), Training deeper convolutional networks with deep supervision, CoRR, abs/1505.02496.