International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Detecting the Security Levels of Various Cryptosystems

M.Thirunavukkarasu[1] , N. Venkatagiri[2], Y. Yaswanth kumar[3]

[1]Assistant Professor, Department of CSE, SCSVMV, Kanchipuram, Tamil Nadu, India
[2]UG Student, Department of CSE, SCSVMV, Kanchipuram, Tamil Nadu, India
[3]UG Student, Department of CSE, SCSVMV, Kanchipuram, Tamil Nadu, India

Abstract- Due to recent evolutions in multimedia technology, the security of digital data has given rise to serious concerns. To label the imperfection of the current security mechanisms, researchers regularly centralize their efforts on changing the existing protocols. However, throughout the past few decades, several proposed encryption algorithms have been manifest to be insecure, posing a major security risk to sensitive data. It is crucial to choose the best encryption method to defend against these attacks, but the type of data being secured will ascertain which algorithm is best in an especial circumstance. On the other hand, evaluating possible cryptosystems one at a time to find the best substitute can take a while. We offer a method for identifying the security level of picture encryption methods that includes a using of support vector machine to choose appropriate encryption methods (SVM) quickly and precisely. In this study, we also develop a dataset containing traditional encryption security norm, such as entropy, contrast, uniformity, peak signal to noise ratio, mean square error, energy, and correlation. These characteristics are gathered from different cypher images as attributes. Three categories—high, acceptable, and weak—are used to categorize the security quality of dataset labels. We evaluated the performance of our proposed model using several studies (f1-score, recall, precision, and exactness) and the results indicate that this SVM-supported system is successful.

Keywords- Cryptosystem, Image encryption, Security analysis, Support vector machine (SVM).

1. Introduction

Security has become a highly sought-after topic of research because of the augmented rise in the communication of multimedia data through unsecure channels (primarily the Internet). New encryption methods are being developed by various experts as a means of shielding data from prying eyes and unwanted users. Diffusion and misunderstanding are two variables that are essential when encrypting digital images (also known as scrambling). Claud Shannon put forth the hypothesis that a safe cryptosystem would have confusion and diffusion techniques. Digital images allow for the direct manipulation of pixels, rows, and columns during the scrambling process, whereas dispersal modifies the authentic pixel values. In other words, every unique pixel value is replaced by the unique value of the S-box throughout the substitution process. However, the data transfer to protect its privacy, an encrypted form is insufficient. For instance, the information included in the switched or elucidated image may still be accessible if an image is encrypted using just one substitution box (S-box). This indicates that the original image cannot be adequately hidden using a single S-box for encryption. [1]- [5].

2. Literature Review

In [1] the authors Hussain, a et.al have proposed a method. Malicious software, or "malware," is a common component of online threats that can even take over a victim's system. Malware frequently uses cryptographic techniques to hide its activities (as in the case of ransom ware). For the time-absorbing conventional methods of binary analysis to be successful, malware and other dangers grow too quickly. In their work, various machine learning methods will be presented for impulsively identifying and designating cryptographic algorithms in binary programmers that have been constructed. To properly evaluate these techniques on binary coders in the realworld, more research is necessary, however the findings in this paper imply that machine learning may be used to detect and recognize cryptographic elementary in compiled code with success. These techniques are now being used to discover and categories' cryptographic procedures in small single-purpose programmers, and more work is being suggested to apply them to real-world situations.

[2] Machine learning approaches to IoT security: A systematic literature review by A. Anees, I. Hussain. As IoT applications continue to grow and change, the number of attacks on those applications also increases quickly. In this systematic literature review (SLR) work, we seek to offer scholars a research resource on current IoT security research trends. This thorough review of the literature on the most recent IoT security articles uncovered a few significant research patterns that will guide this field's future study. It's critical to create models that can incorporate cutting-edge methods and tools from big data and machine learning given the exponential increase of large-scale IoT threats. Finding the appropriate algorithms and models to identify IoT attacks in real-time or close to real-time requires a focus on accuracy and efficiency. [3] A. Shafique's methodical review of the literature on machine learning and cryptographic algorithms. Ransomware and vulnerabilities detection analysis and design. The machine learning approach that is suggested in this work can be used

to model the new ransomware detection and the random number decryption techniques for the new model to break the encryption for recovering the ransom. According to the study, a machine could distinguish between infectious and non-viral data using a trained model. The main problem has been structurally broken down into the sub problems of ransomware problem identification and designing cryptographic algorithms based on machine learning to produce the decryption key for the ransom problem.

2.1 Existing System

Obtaining a completely balanced and highly connected dataset in the current system is nearly impossible. Despite the vast amounts of data accessible, collecting relevant data is a difficult task. To get around this, we use the scikit-learn library's machine learning tools to extract meaningful data.

Disadvantages

- High Complexity
- Very long encrypting time

2.2 Proposed Method

There has been a tonne of new encryption algorithms developed recently, such as chaotic and transformation-based systems. Numerous encryption algorithms, such as chaotic and transformation-based ones, have been introduced in recent years. It has been determined through statistical analysis of existing encryption algorithms that some of them are unconfident and do not provide appropriate protection. [7] One way for determining the security level of an encryption procedure is to examine the statistics of its security parameters. Making these collations one by one, which takes a long time, is a traditional technique of accomplishing this. To assist us identify an appropriate encryption strategy more swiftly, we designed a machine learning system that combines SVM. [9]

Advantages

- Less Complexity
- It increases the accuracy.

2.3 Architecture

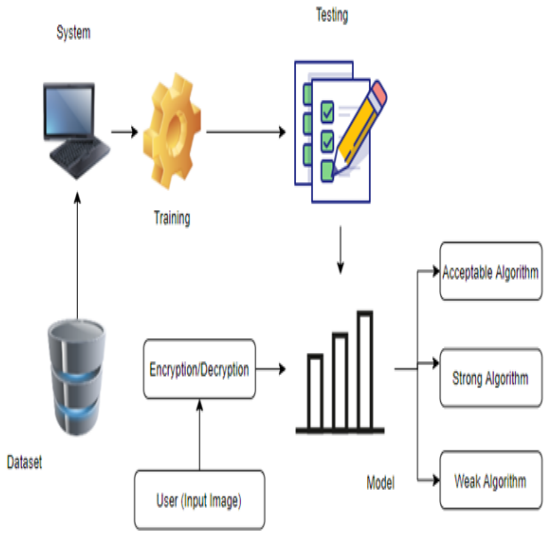

Figure 1. Architecture of Data Processing

According to the architecture shown in Figure 1. the dataset first gathers a variety of encrypted image data types before converting each one into a different data list. Following the conversion of the data list, the concoction of the data is split up into two stages: training data and testing data. After the data set has been prepared, it begins to examine the dataset labels' security levels and determines if the encrypted image data's security is high, acceptable, or low based on the chosen techniques.

2.4 Modules

Data collection: Information or data must be gathered from open sources, which will be used to train the models.

Pre-processing: Data must be pre-processed according to the models in order to improve the model's accuracy and provide more information about the data. Feature Engineering: In this step, features are chosen depending on the importance of the column data, allowing us to spend less time on multiple columns.

Model Building: Model building for the dataset is a key stage in obtaining the ultimate outcome. We create a classification and regression model based on the data.

View Results: The user can see the model's generated results.

Model Checking: System checks model accuracy, and it takes of the necessary for the model building

Generate Results: System takes the input data from the users and produces the output. So that we can receive the result in this method.

2.5 Algorithm

Support-vector machines, or SVMs for short, are supervised learning models that analyze data using learning algorithms for classification and regression analysis. One of the most effective methods for prediction is the use of SVMs, which are based on statistical learning frameworks. Given a set of training examples, each of which is labelled as belonging to one of two categories, an SVM training method builds a model that assigns future examples to one of two categories, resulting in a non-probabilistic binary linear classifier. To create as large of a gap between the two categories as possible, SVM translates training examples to points in space. Then, new examples are mapped into that same area and projected to fall into a particular category based on which side of the gap they are located.

For classification, regression, or other tasks like outlier detection, a support-vector machine, or SVM, builds a hyper plane or group of hyper planes in a high- or infinite-dimensional space. Intuitively, the hyper plane with the greatest separation from the closest training data point of any class (referred to as the functional margin) separates rather well since the wider the margin, the smaller the generalization error of the classifier. The sets to discriminate are typically not linearly separable in the first problem's finite-dimensional space, despite that space being the initial problem's expression. Due to this, it was proposed [5] that the original finite-dimensional space be transplanted into a much higher-dimensional area, ostensibly making separation there easier.

By specifying the mappings employed by SVM methods in terms of a kernel function, it is ensured that the dot products of pairs of input data vectors may be computed easily in terms of the variables in the original space. An approach for supervised machine learning called the Support Vector Machine (SVM) is utilized for both classification and regression. Even if we also refer to regression issues, classification is the best fit. It seeks to identify natural grouping of the data and then maps new data to these established groups. Hava Siegelmann and Vladimir Vapnik's support vector clustering [2] technique uses the support vector statistics produced in the support vector machines approach to classify unlabeled data. In order to create the hyperplane, SVM selects the extreme points and vectors. Not only do support vector machine models accept sparse data well, but they can also categorize groups of data or generate predictive rules for data that cannot be classified by linear decision functions, making them an effective tool for identifying predictive models or classifiers. SVMs are complicated in part because they were designed to produce classifiers based on all available variables at the time and did not permit the evaluation of variable significance. Both input and output data are provided by them.

2.6 Implementation

Because of its step-by-step implementation process, our project uses the waterfall model as its software development cycle.

Requirement Gathering and analysis: In this stage, every potential requirement for the system that will be created is gathered and outlined in a requirement specification document.

System Design: In this phase, the required specifications from the first phase are examined, and the system design is created. This system design aids in determining the overall system architecture as well as the hardware and system requirements.

Implementation: The system is initially built in tiny programmers known as units with input from the system design, and is then combined in the following phase. Unit testing is the process of creating each unit and evaluating it for functionality.

Integration and Testing: After each unit has undergone testing during the implementation phase, the entire system is merged. Following integration, the entire system is examined for errors and failures.

Deployment of system: Following completion of both functional and non-functional testing, the product is either made available for purchase or implemented in the customer's environment.

Maintenance: In the client environment, certain complications can arise. Patches are made available to resolve certain problems. Better versions of the product are also released in order to improve it. These modifications are sent to the customer environment through maintenance.

3. Results

A methodology has been implemented that can accurately and rapidly ascertain the security level of various encryption techniques. The dataset has been builded and adding characteristics to it that included the security framework that are common to various encryption models. The values of all accredits are separated into three intervals- strong, acceptable, and weak- to generate a dataset that describes the resulting security levels. Then the security levels can also be detected using statistical statics. The execution of the model has been finally assessed and checked the performance using many trails. This proposed mothed does not takes a long time. The different encryption systems are tested to see what level of security is provided.

Finally, the accuracy of every image will be showed in the page.

3.1 Machine Learning Models for detecting the security level of various cryptosystems:

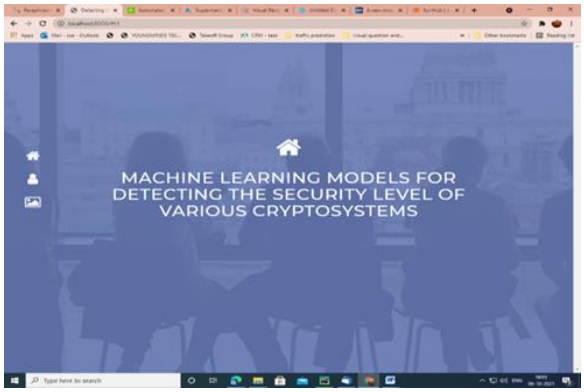

Figure 2. Home page for detecting the security levels of various cryptosystems.

This results the front page of the website. It presents three icons. The home icon shows the title of detecting the security level of various cryptosystems. We can go through the further steps form detecting the security level using the machine learning models.

3.2 This page describes the concept behind this project.

Of varpous

Figure 3. Description about the project

In this page we can find the concept behind this project. We can see the concept about the machine learning models that have been used for detecting the security level of various cryptosystems. It shows the information about the need for using support vector machine algorithm for detecting the security level of various cryptosystems.

3.3 This page describes the accuracy of all models.

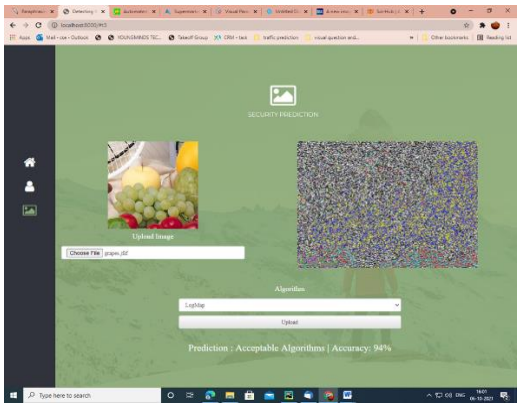

Figure 4. Accuracy of all models

In this result we will be uploading the image to find the security level of that image. Support Vector Machine algorithm performs it functions and finds the security level. So, this page describes the accuracy of all models.

3.4 Test Cases

Table 1. Test Cases of the Security Levels

Input	Output	Result
Input features	Tested on many models for various features supplied by users.	Success
Security Levels Classification	Different techniques and data are used to generate the models, which are then tested for various input features provided by the user on various model features.	Success
Security Levels Prediction	In order to estimate security levels, various models derived from algorithms will be used.	Success

4. Conclusion

In this study, we have extended a model that can quickly, readily, and precisely determine the security level of different encryption algorithms. We started by building a dataset and adding characteristics that represented the security parameters shared by different encryption techniques. In order to create a dataset, we divided all feature values into three intervals—strong, acceptable, and weak—that represent the aforementioned security categories. Next, our suggested model is used to test various encryption techniques in order to gauge their level of security. By calculating the statistical values of each, we can manually determine the security level of these encryption techniques. This procedure takes a long time to complete using standard testing techniques, but with our suggested approach, testing may be completed in a matter of seconds. In conclusion, we also evaluated the performance of our suggested model using various tests, and we found that it generates 94% accurate predictions at significantly faster rates than other models now in use. Finally, utilizing numerous trails to assess and validate the performance of our suggested model, we found that it delivers 94% accurate predictions at a noticeably faster rate. Future testing will closely examine the use of deep learning techniques to determine the level of security of cryptosystems.

References

[1] I. Hussain, A. Anees, Et al., ‘‘Image encryption based on Chebyshev chaotic map and S8 S-boxes,” *Optica Applicata.*, pp. 317-330 (2019)

[2] A. Anees, I. Hussain, Et al., ‘‘A robust watermarking scheme for online multimedia copyright protection using new chaotic map,’’*Secur. Commun. Netw.*, pp. 1-20 (2018)

[3] A. Shafique, Et al., ‘‘Dynamic substitution-based encryption algorithm for highly correlated data,” *Multidimensional Syst. Signal Process.*, pp. 91-114 (2020)

[4] F. Ahmed, A. Anees, Et al., ‘‘A noisy channel tolerant image encryption scheme,’’*Wireless Pers. Commun.*, pp. 2771-2791 (2014)

[5] M. A. B. Farah, R. Guesmi, Et al., ‘‘A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation,” *Opt. Laser Technol.*, pp. 56-57 (2019)

[6] C. E. Shannon, Et al., ‘‘Communication in the presence of noise,” *Proc.* IEEE, pp. 1192-1201 (1949)

[7] S. Heron, ‘‘Advanced encryption standard (AES),’’*Netw. Secur.*, pp. 8-12 (2009)

[8] H. Liu, Et al., ‘‘Chaos-based fast colour image encryption scheme with true random number keys from environmental noise,’’*IET Image Process.*, pp. 324-332 (2017)

[9] Y.-L. Lee, Et al., ‘‘A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible colour transformations’’*IEEE Trans. Circuits Syst. Video Technol.*, pp. 695-703 (2018)

[10] A. Anees, Et al., ‘‘Chaotic substitution for highly autocorrelated data in encryption algorithm,’’*Commun. Nonlinear Sci. Numer. Simul.*, pp. 3106-3118 (2014)

[11] L. Liu, Et al., ‘‘A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation,’’ *IEEE Access*, pp. 27361–27374, (2020)

[12] M. Khalili, Et al., ‘‘Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold trans-form map,’’ *IET Signal Process*., pp. 177–187, (2021)

[13] L. Zhang, Et al., ‘‘Image encryption with discrete fractional cosine transform and chaos,’’ in *Proc. 5th Int. Conf. Inf. Assurance Secure*., pp. 61–64. (2009)

[14] M. Zhang, Et al., ‘‘Image compression and encryption scheme based on compressive sensing and Fourier transform,*’’ IEEE Access*, pp. 40838–40849. (2020)

[15] J. S. Khan, W. Boulila, Et al., ‘‘DNA and plaintext dependent chaotic visual selective image encryption,’’ *IEEE Access*, pp. 159732–159744. (2020)