International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

DETECTING THE SECURITY LEVEL OF VARIOUS CRYPTOSYSTEMS USING MACHINE LEARNING MODELS

B.Manjunath[1], K.S.Phaneendra[2], M.Gowrish[3]

[1,2,3] *Pg Scholar Department Of computer of application*
[1,2,3]*Madanapalle Institute of Technology and Science , Andhra Pradesh, 517352*

Abstract - The security of digital data has become a huge concern as a result of recent advances in multimedia technology. Researchers tend to focus their efforts on changing existing protocols to overcome the flaws of present security mechanisms. Several proposed encryption algorithms, however, have been proven insecure during the last few decades, posing serious security risks to sensitive data. Using the most appropriate encryption technique to protect against such assaults is critical, but which algorithm is most suited in any given situation will depend on the type of data being secured. Testing potential cryptosystems one by one to identify the best alternative, on the other hand, can take a long time. . We present a security level identification approach for picture encryption algorithms that incorporates a support vector machine for a fast and accurate selection of relevant encryption algorithms (SVM). We also generate a dataset with conventional encryption security criteria like entropy, contrast, homogeneity, peak signal to noise ratio, mean square error, energy, and correlation in this research. These parameters are collected from various cypher pictures as features. The security level of dataset labels is categorised into three categories: high, acceptable, and weak. We used various studies (f1-score, recall, precision, and accuracy) to assess the performance of our suggested model, and the findings show that this SVM-supported system is effective.

Keywords: Support vector machine (SVM), security analysis, image encryption, cryptosystem.

1. INTRODUCTION

Security has become a much-in-demand topic of research because to the exponential increase in transmissions of multimedia data across insecure channels (primarily the Internet). Many researchers have turned to inventing new encryption methods to safeguard data from eavesdroppers and unauthorised users [1]–[5]. Two elements are critical when encrypting digital images: diffusion and confusion (also known as scrambling). Claud Shannon proposed in [6] that a cryptosystem that includes confusion and diffusion methods can be regarded secure. The scrambling process on digital images can be done directly on pixels or on rows and columns, whereas diffusion affects the original pixel values. In other words, the substitution procedure substitutes each unique pixel value with the S-unique box's value. The transmission of data in an encrypted format, however, is insufficient to preserve its privacy. For example, if a single substitution box (S-box) is used to encrypt an image, the information in the substituted or enciphered image may still be visible. This means that a single S-box encryption is insufficient to properly conceal the source image. Despite the fact that the information being communicated is encrypted, unauthorised individuals can still view it due to the encryption algorithm's flaws, as seen in Figure 1. (b). Thus. To improve encryption security, it is also vital to utilise a strong encryption algorithm. The security level of the encryption algorithm used to encrypt the image has a significant impact on its robustness. The plain image will be entirely encrypted using a highly strong encryption method, allowing it to withstand attacks on its integrity, secrecy, and availability. Along with security, temporal complexity is a significant consideration when choosing an effective encryption method. Because different types of data have different security priorities, choosing a cryptosystem is dependent on the nature of the application to be encrypted. The Advanced Encryption Standard (AES) [7] is, for example, the most secure encryption algorithm available at the moment. However, because AES requires numerous rounds, which takes longer, it is not suited for applications that demand quick encryption. The original information must be encrypted, which takes additional time. Furthermore, the total number of pixels in the source image influences the temporal complexity. The higher the amount of pixels in the plain image, the longer it will take to encrypt it [8]. If the main requirement is simply to encrypt a plain image with high security, on the other hand, processing time may not be as important. Although strong encryption gives superior security, it is not always a property of quick encryption, which is sometimes preferred [9]. A statistical study such as entropy, correlation, energy, or homogeneity must be done on an encryption algorithm to determine its security level. Testing each encryption technique and calculating the statistics of its security characteristics can help with these duties. We can choose the best and strongest choice from those examined after completing such security studies on each encryption method one by one. However, this procedure frequently detracts from the completion of the assignment. Instead, we recommend that manual testing be replaced by a machine learning model that can quickly, easily, and accurately identify the strongest encryption technique. Based on conventional security factors of encryption algorithms, we have classified the security of encryption algorithms into three levels (strong, moderate,

and weak). The details of how we split encryption methods into three security categories based on security criteria like entropy, homogeneity, contrast, correlation, energy, PSNR, and MSE are detailed below. We're focusing on the encryption techniques that are utilised to encrypt 8–bit images. The maximum entropy for 8–bit pictures cannot be surpassed by 8. Similarly, the greatest entropy that can be computed for binary images is 2. As a result, in the instance of 8-bit pictures, the entire entropy interval has been partitioned into three intervals. The entire interval ranges from 0 to 8. Any plain image's average entropy value can range from 7.600 to 7.700. An encrypted image formed with a poor encryption method such as a single Substitution-box (S-box) algorithm, on the other hand, may have an average entropy value of 7.9503 to 7.9799. The average entropy value for an adequate and strong encryption technique might range from 7.9800 to 7.9900 and 7.9901 to 8.000, respectively. Other security parameters' values may also change as a result of this. We collect the security parameter values for several encrypted images generated by different encryption techniques to justify the preceding conclusion. The photos cannot be adequately encrypted using weak and moderate encryption techniques. Figure 3 shows the decrypted photos encrypted with weak and intermediate encryption techniques. Table 1 shows the statistical statistics for several images encrypted with weak, moderate, and strong encryption techniques, as well as the related average entropy values. We evaluated all sorts of picture encryption techniques for security level detection, including frequency domain, transform-based, and chaotic maps-based schemes. The suggested work's main goal is to determine the encryption techniques' security level. To create a dataset, we looked at a number of encrypted photos and extracted their feature values. The dataset's size is unrestricted; it can be of any size. The dataset must provide feature values for both high and acceptable security levels. Take entropy values as an example; we used a step size of 0.0001 for the entropy values. The entropy values have been separated into three intervals. There are one hundred values ranging from 7.9901 to 8.000 for robust security. Similarly, the acceptable security level has a range of 102 values ranging from 7.9900 to 7.9800. All other numbers less than 7.9800 indicate a low level of security. Similarly, we separated the other parameter values into three intervals by selecting a step size that was adequate. Table 2 shows a piece of the proposed dataset in which the first twenty feature vectors of each category of security level are displayed for viewing purposes. Classification guidelines

• The range of each parameter has been separated into three intervals: weak, acceptable, and good security. Below 50% of feature values must be in the permitted interval values for the weak security level.

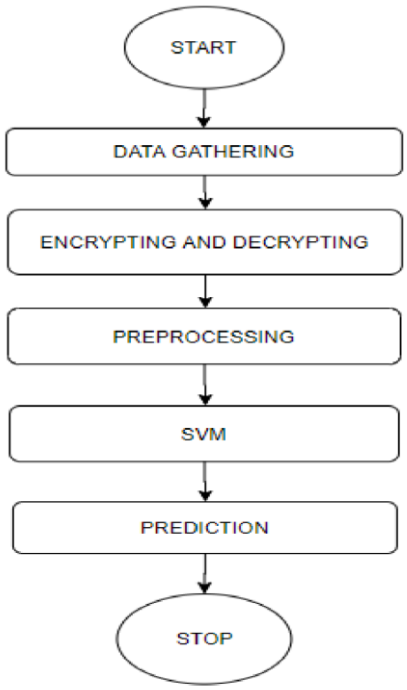
• At least 65 percent of feature values must fall inside the permitted interval values for acceptable security.

LITERATURE REVIEW

A number of encryption techniques have been presented as ways to secure photos before they are transmitted. Chaos or transformation methods, such as discrete wavelet transformation, discrete cosine transformation, and discrete Fourier transformation, may be used to build encryption algorithms [12]–[17]. However, these are just a few of the many image encryption algorithms proposed in recent years. The following sections provide more information on each type: An picture encryption technique based on cosine transformation and chaos was proposed in [18]. Instead of a single chaotic system, three separate chaotic maps were used. The idea behind employing more than one chaotic map was to add complexity to the entire algorithm, allowing it to behave in more complex and dynamic ways. Kaur et al introduced a new optical image encryption approach based on a chaotic in [19], which demonstrated capable of creating vectors of different orders using a piece-wise linear chaotic map (PWLCM) [20] to improve the security of the encryption process. Khan et al. introduced a chaos-based selective picture encryption technique in [21] for rapid image encryption. Although selective encryption systems work well for real-time applications that demand quick encryption, they are not suited for text encryption, where every single bit must be encrypted in order for the data to be effectively concealed. The statistical analysis showed that these algorithms accomplished efficient encryption; nonetheless, these results were insufficient to demonstrate the proposed work's security level. More research is needed to give a more accurate assessment of that encryption algorithm. Despite the fact that chaos can generate random numbers, Nardo et al. explained the limitations of chaos-based encryption schemes in [22], claiming that these types of encryption algorithms are implemented on a finite precision computer, resulting in dynamic degradation, making chaos-based encryption insecure. The authors used a finite precision error to encrypt plain images, which was generated by implementing chaos-based systems with varied interval delays. In [23], the authors asserted that chaos-based communication systems are not safe enough since they rely on beginning values, which means that their security can be compromised by identifying those initial values. In our previous work, we used a bit-plane extraction approach to propose a novel image encryption methodology based on multiple chaotic systems [24] to improve the security of the chaos-based cryptosystem. The proposed technique's major goal was to shorten the processing time while also improving the amount of concealment available. [10] proposes an image encryption technique based on a chaotic logistic map (CLM) [25]. The author of this paper addressed the problems with single substitution box (S-box) encryption by employing multiple S-box image encryption, where the selection of a particular S-box is determined by the CLM's random values. S-boxes are a common component in chaos-based picture encryption due to its powerful, nonlinear diffusion source. S-boxes are therefore crucial in converting

the original data into an encoded representation. Because the robustness of chaos-based encryption methods is dependent on the S-box, this component must be able to withstand statistical attacks. For security specialists, developing powerful S-boxes is a crucial study field. We earlier presented a CLM-based methodology capable of building a new S-box in [26] to overcome the concerns with employing weak Sbox. A little change in the initial values of CLM may cause the values of the S-box to alter. Apart from grayscale picture encryption, colour image encryption is even more difficult than grayscale image encryption. This is due to the fact that colour image encryption The R, G, and B channels must all be encrypted. [27] proposes a colour image encryption approach based on a hybrid chaotic system. The authors employed the occurrence of confusion to encrypt each R, G, and B component separately, then diffused the confused components using a mitochondrial DNA sequence. Each of the above-mentioned encryption algorithms has a distinct level of security: some are strong, others are acceptable, and some are weak. The complexity of an algorithm's mathematical structure determines which category it belongs to.

Block diagram:



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
- Time consuming.

Proposed system:

In recent years, a flood of encryption algorithms have been introduced, including chaos and transformation-based methods. It has been determined through statistical analysis of existing encryption algorithms that some of them are insecure and do not provide appropriate protection. One way for determining the security level of an encryption algorithm is to examine the statistics of its security parameters. Making these comparisons one by one, which takes a long time, is a traditional technique of accomplishing this. To assist us identify an appropriate encryption strategy more quickly, we designed a machine learning model that combines SVM.

Advantages:

- Less complexity.
- Time consuming

Implementation:

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.

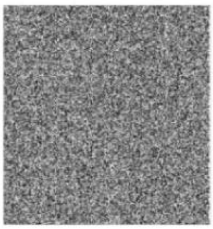
Feature Engineering: In this step, features are chosen depending on the importance of the column data, allowing us to spend less time on multiple columns.

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.

Result:

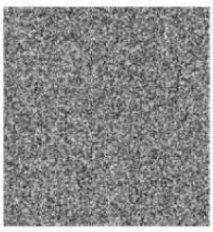
(a) Plain Cameraman image



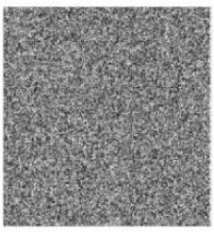
(b) Encrypted image using encryption scheme proposed in [21]

(c) Encrypted image using encryption scheme proposed in [10]

(d) Single S-box encryption



(e) Encrypted image using encryption scheme proposed in [29]



(f) Encrypted image using encryption scheme proposed in [30]

Conclusion:

We created and proposed a methodology in this paper that can accurately and rapidly detect the security level of various encryption techniques. We started by building a dataset and adding characteristics to it that included the security parameters that are common to various encryption techniques. We separated the values of all attributes into three intervals—strong, acceptable, and weak—to generate a dataset that describes the resulting security levels. The different encryption systems are then tested on our proposed model to see what level of security they provide. We can also manually detect the security level of these encryption techniques by calculating their statistical statistics. This process takes a long time with standard testing methods, but with our proposed model, testing may be completed in a matter of seconds. Finally, we evaluated and checked the performance of our suggested model using many trials, and we discovered that it provides 98 percent correct predictions at significantly faster speeds than other models now available. The application of deep learning algorithms to detect the security level of cryptosystems will be examined in future research.

References:

[1] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, ‘‘Image encryption based on Chebyshev chaotic map and S8 S-boxes,’’ Optica Applicata, vol. 49, no. 2, pp. 317–330, 2019.

[2] A. Anees, I. Hussain, A. Algarni, and M. Aslam, ‘‘A robust watermarking scheme for online multimedia copyright protection using new chaotic map,’’ Secur. Commun. Netw., vol. 2018, pp. 1–20, Jun. 2018.

[3] A. Shafique and J. Ahmed, ‘‘Dynamic substitution based encryption algorithm for highly correlated data,’’ Multidimensional Syst. Signal Process., May 2020.

[4] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, ‘‘A noisy channel tolerant image encryption scheme,’’ Wireless Pers. Commun., vol. 77, no. 4, pp. 2771–2791, Aug. 2014.

[5] [5] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, ‘‘A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation,’’ Opt. Laser Technol., vol. 121, Jan. 2020, Art. no. 105777.

[6] [6] C. E. Shannon, ‘‘Communication in the presence of noise,’’ Proc. IEEE, vol. 72, no. 9, pp. 1192–1201, Sep. 1984.

[7] S. Heron, ‘‘Advanced encryption standard (AES),’’ Netw. Secur., vol. 2009, no. 12, pp. 8–12, Dec. 2009.

[8] H. Liu, A. Kadir, and X. Sun, ‘‘Chaos-based fast colour image encryption scheme with true random number keys from environmental noise,’’ IET Image Process., vol. 11, no. 5, pp. 324–332, Apr. 2017.

[9] Y.-L. Lee and W.-H. Tsai, ‘‘A new secure image transmission technique via secret-fragmentvisible mosaic images by nearly reversible color transformations,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 4, pp. 695–703, Apr. 2014.

[10] A. Anees, A. M. Siddiqui, and F. Ahmed, ‘‘Chaotic substitution for highly autocorrelated data in encryption algorithm,’’ Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 9, pp. 3106– 3118, Sep. 2014.