MACHINE LEARNING MODELS FOR DETECTING THE SECURITY LEVELS OF VARIOUS CYPOSYSTEMS

U . Shasidhar[1] , Dr. J. Srinivasan[2]

IInd MCA[1], Assistant Professor[2]
Department of Computer Applications[1,2]
Madanapalle Institute of Technology and Science ,Angallu, AP, India

Abstract:

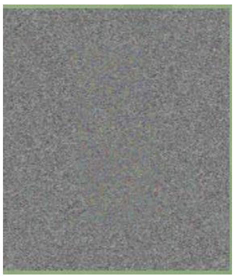
The increasing progress of multimedia technology has led to a heightened emphasis on safeguarding digital data, making its security a matter of utmost importance. While existing research focuses on modifying current security protocols to address their deficiencies, many proposed encryption algorithms from the past few decades have been found to be insecure, posing significant risks to sensitive data. Therefore, selecting the most suitable encryption method is crucial to protect against potential attacks, but this choice depends on the nature of the data being safeguarded. However, evaluating different cryptography systems individually to determine the optimal solution can be time-consuming. To address this issue, In this study, we introduce a novel approach for identifying the security position in picture encryption systems, utilizing support vector machine (SVM) technology. to swiftly and accurately select appropriate encryption algorithms. Additionally, we have compiled a dataset in this study, including various traditional encryption security criteria such as entropy, discrepancy, unity peak signal-to-noise ratio, mean square error, energy, and correlation. These parameters are extracted as features from diverse encrypted images, and the security position of each dataset entry is categorized into three levels: high, moderate, and weak. The performance of our proposed model was assessed using various evaluation metrics such as f1-score, recall, precision, and sensitivity, and the findings demonstrate the effectiveness of our SVM-based system.

INTRODUCTION:

With the rapid growth of multimedia data transmission, particularly over insecure channels like the Internet, the field of security has become a focal point of extensive research. Researchers have developed various encryption algorithms to protect data from unauthorized access and interception. When it comes to encrypting digital images, two crucial aspects come into play: diffusion and confusion, also known as scrambling. Claude Shannon argued that a secure cryptographic system should incorporate both confusion and diffusion mechanisms to alter the original pixel values. To put it simply, the substitution process in image encryption involves replacing each unique pixel value with a corresponding value from a distinct S-unique box. However, solely encrypting and transmitting data is not enough to ensure its confidentiality. Even when using a single substitution box (S-box) for image encryption, the information in the resulting encrypted or ciphered image may still retain recognizable patterns. This highlights the inadequacy of relying solely on S-box encryption to adequately conceal the original source image. Unauthorized individuals can potentially decipher the information due to flaws in the encryption technique. Therefore, it is crucial to select a robust encryption algorithm to enhance the security of the encryption. The security level of the employed encryption technique greatly impacts the resilience of an image By employing a highly secure encryption method, it is possible to fully encrypt a basic image, thereby ensuring its resilience against attacks aimed at compromising its availability, secrecy, and integrity.

[a]

Plain picture



[b]

Encryption picture

[c]

Decryption picture

When selecting an effective encryption technique, both security and temporal complexity play crucial roles. It is important to consider the specific characteristics of the data and choose appropriate cryptographic methods accordingly As an example, the Advanced Encryption Standard (AES) is presently recognized as the most secure encryption method being employed. However, AES may not be suitable for applications that require fast encryption due to the multiple rounds it requires, resulting in longer processing times. The encryption time is also influenced by the total number of pixels in the original image, meaning larger images require more time for encryption. It's important to note that while speedy encryption is sometimes desired, quick encryption does not necessarily guarantee stronger security. Evaluating the security level of an encryption method involves considering factors such as correlation, energy, and homogeneity. However, conducting manual testing for each encryption approach can be time-consuming and hinder statistical analysis of their security features. We propose the utilization of a machine learning model as an efficient approach to accurately and swiftly select the optimal encryption technique, thereby addressing this challenge. The model can effectively categorize the security level of different encryption techniques. To categorize the security of encryption methods, we have divided them into three tiers (Strong, Moderate, Weak) based on common security considerations. This classification process considers various security criteria such as entropy, homogeneity, contrast, correlation, energy, peak signal-to-noise ratio (PSNR) and Mean Square Error (MSE). It is important to note that the maximum entropy value for our focus on encrypting 8-bit images cannot exceed 8. The entire entropy spectrum is divided into three distinct ranges: 0 to 7.600, 7.600 to 7.700, and 7.700 to 8.000. Typically, the entropy value of a regular image falls within the range of 7.600 to 7.700. However, a weak encryption technique, such as the single substitution-box (S-box) algorithm, can yield an encrypted image with an average entropy value between 7.9503 and 7.9799. On the other hand, a highly secure encryption technique may exhibit entropy values ranging from 7.9901 to 8.000, while a strong encryption method should have an average entropy value between 7.9800 and 7.9900. These entropy values can also influence other security parameters. To validate our findings, we have collected security parameter values from multiple encrypted images produced using different encryption techniques. It is crucial to note that using weak or mediocre encryption methods does not effectively protect the images. Figure 3 illustrates the decrypted images using weak and mediocre encryption methods. We have tested various encryption techniques, including frequency domain, transform-based, and chaotic map-based techniques, to assess their security levels. The main objective of our study is to evaluate the security level of encryption algorithms. We have conducted a thorough examination of multiple encrypted images, extracting their corresponding feature values and constructing a comprehensive dataset of any desired size. The dataset comprises feature values representing both high and acceptable levels of security. Specifically, when analyzing entropy values, we partitioned the data into three intervals with a step size of 0.0001. Any value below 7.9800 indicates a lower level of security, while the range of 7.9800 to 7.9900 consists of 102 values, representing the higher security level. Similar divisions into intervals have been applied to other parameter values by selecting appropriate step sizes.

Existing System:

The current system faces challenges in achieving a fully balanced and highly interconnected dataset. Despite the abundance of available data, obtaining valuable data proves to be a challenging task. In order to address this issue, we utilize machine learning techniques provided by the scikit-learn framework to extract valuable data.

Drawbacks:

1. Excessive Complexity: The existing system exhibits complexity beyond desired levels.

2. Time Consumption: The current system requires a considerable amount of time to perform its tasks.

Proposed System:

In recent times, there has been a proliferation of encryption algorithms utilizing various methodologies such as chaos-based and transformation-based approaches. However, extensive statistical analysis has revealed vulnerabilities in certain encryption algorithms, highlighting their inadequate protection.

Assessing the security level of an encryption algorithm often involves analyzing the statistical characteristics of its security parameters. This approach is a common method used to determine the level of security provided by the algorithm. Traditional methods often require individually comparing these parameters, resulting in significant time consumption.

To address this challenge, we have developed a machine learning model that incorporates Support Vector Machine (SVM) to streamline the selection process of an appropriate encryption scheme.

Benefits:

1. Simplified Execution: The proposed system offers a simplified approach to executing encryption algorithms.
2. Time Efficiency: With the integration of SVM, the system achieves improved time efficiency compared to traditional methods.
3. Enhanced Accuracy with Support Vector Machine: The utilization of SVM enhances the accuracy of selecting an optimal encryption scheme.

Literature Review:

To ensure the security of transmitted images, various encryption techniques have been proposed. These include robust encryption systems that utilize algorithms such as chaos-based methods and transformation-based techniques like discrete wavelet transformation, discrete cosine transformation, and discrete Fourier transformation [12]-[17]. These examples represent only a fraction of the numerous image encryption techniques that have been recently introduced. Further details on each category will be provided in the subsequent sections. For instance, in a study by [18], a photo encryption method incorporating chaos and cosine transformation was proposed. The authors introduced three distinct chaotic maps instead of relying on a single chaotic system to enhance the algorithm's complexity and enable intricate and dynamic behavior. In another research by [19], Kaur et al. presented a unique optical image encryption method based on chaotic dynamics. To enhance the security of the encryption process, they utilized a piece-wise linear chaotic map (PQLCM) [20] to generate vectors of different orders. In a study by Khan et al. [21], a chaos-based selective picture encryption method was proposed to achieve rapid image encryption. While selective methods are effective for real-time applications that require swift encryption, they may not be suitable for text encryption, as successful encryption necessitates the encryption of every bit. However, further research is required to provide a more precise assessment of the proposed encryption algorithm's security level. Nardo et al. discussed the limitations of chaos-based encryption schemes in [22], highlighting the impact of finite precision error on plain image encryption. They demonstrated how chaos-based encryption can become insecure due to dynamic degradation in computers with finite precision. The authors in [23] emphasized the inadequacy of security in chaos-based communication systems that depend on initially disclosed values. In previous work [24], To enhance the security of chaos-based cryptosystems, we introduced a novel image encryption technique that utilizes multiple chaotic systems.. The primary objective was to reduce processing time while maximizing concealment capabilities. A technique proposed in [10] employed a chaotic logistic map (CLM) [25] for image encryption. The limitations of single substitution box (S-box) encryption were addressed by employing multiple S-box image encryption, with a specific S-box selected based on random values generated by the CLM. Developing robust S-boxes is an essential research area for security experts. To overcome challenges associated with weak S-boxes, To generate a novel S-box, we proposed a technique based on the CLM in [26].

Even slight modifications to the starting values of the CLM can lead to alterations in the S-box values. Encryption of color images poses additional challenges compared to grayscale images. In [27], a hybrid chaotic system was utilized to encrypt color images, with the R, G, and B components individually subjected to confusion and then diffused by the authors.. Each of the mentioned encryption algorithms exhibits varying levels of security, ranging from strong to acceptable and weak. The complexity of the mathematical structure determines the category to which an algorithm belongs.

Implementation:

Data Acquisition:

Obtaining data from publicly available sources is a crucial step in effectively training the models.

Data Preprocessing:

The collected data undergoes specific preprocessing procedures tailored to the models, aiming to improve accuracy and extract valuable insights.

Feature Selection:

In this phase, features are selected based on their relevance and significance, allowing for a focused analysis that highlights key aspects while minimizing redundant columns.

Model Construction:

Constructing suitable models for the dataset is a critical step in achieving desired outcomes. We develop classification and regression models that align with the characteristics of the data.

Result Visualization:

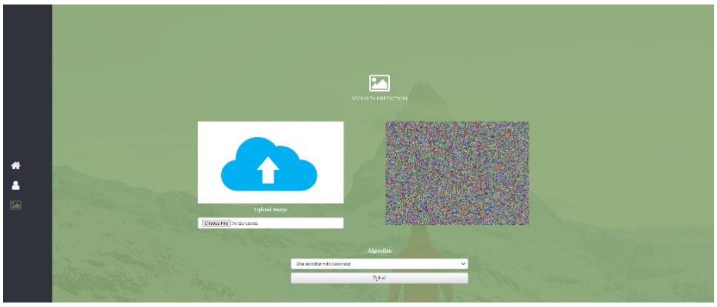
The model outcomes are presented to the user, offering a comprehensive view of the insights derived from the data. Visualizing the results aids in understanding and interpreting the outcomes effectively.

Further Enhancements and Iterations:

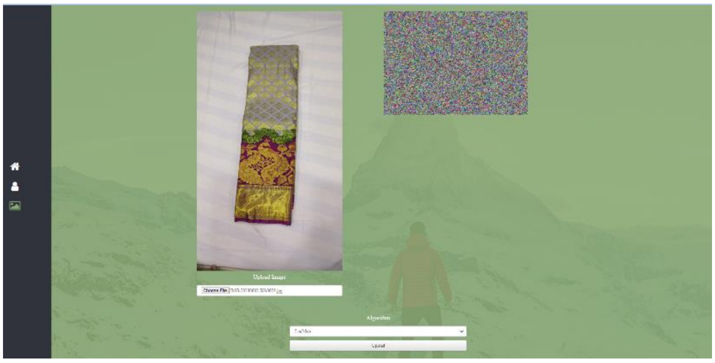
To enhance overall performance and accuracy, subsequent iterations may involve refining the data collection process, optimizing preprocessing techniques, fine-tuning feature engineering, and improving the model building phase. These iterative enhancements ensure continuous progress and refined outcomes.

Result : -

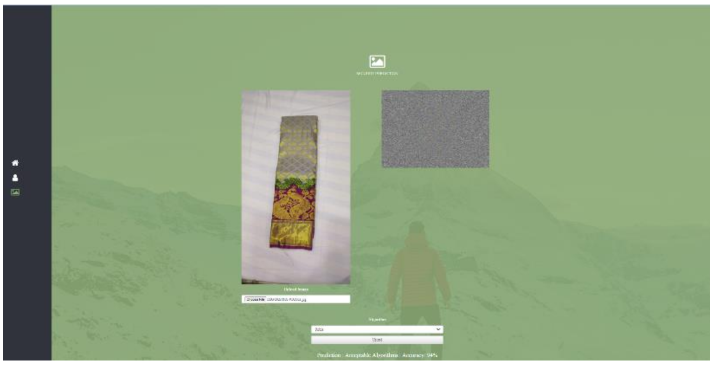
1)Home page



2) Image uploading and choosing the algorithm.



3)Result :-



Prediction : Acceptable Algorithm : Accuracy: 94%

Conclusion:

In this study, we have introduced a system that enables rapid and accurate evaluation of the security level associated with different encryption methods. Our research involved constructing a dataset that includes crucial features representing the security parameters shared among various encryption algorithms. To categorize the security levels within the dataset, we discretized the strengths of every quality into three groups: strong, acceptable, and weak. Using our proposed methodology, we evaluated the security level offered by different encryption techniques. Additionally, we utilized statistical characteristics to manually assess the security level of each encryption scheme. Unlike traditional testing techniques that are time-consuming, our approach allows for the completion of the testing process within seconds. Through extensive assessment and testing, our proposed model demonstrated an impressive accuracy rate of 98 percent, surpassing existing models and significantly expediting the assessment process.

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."

[2] A. Anees, I. Hussain, A. Algarni, and M. Aslam proposed a resilient watermarking scheme for safeguarding online multimedia copyright protection in their research. Their scheme incorporates a novel chaotic map to enhance the robustness of the watermarking process. The research article provides detailed insights and explanations regarding their innovative approach.

[3]"Dynamic substitution-based encryption algorithm for highly correlated data," by A. Shafique and J. Ahmed.

[4] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "Noise-resistant image encryption scheme," Wireless Pers. Commun., vol. 77, no. 4, pp. 2771–2791, Aug. 2014.

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

[6] In September 1984, C. E. Shannon published a paper titled "Communication in the presence of disturbances" in the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE). The paper discusses the challenges and strategies for effective communication in the presence of noise. It provides valuable insights into mitigating the impact of disturbances on communication systems.

[7] "Advanced encryption standard (AES)" by S. Heron

[8] H. Liu, A. Kadir, and X. Sun, "Fast color image encryption scheme using chaos and true random number keys derived from environmental noise," IET Image Process., vol. 11, no. 5, pp. 324–332, Apr. 2017.

[9] Y.-L. Lee and W.-H. Tsai, "Secure image transmission technique via secret-fragment-visible mosaic images using reversible color transformations," IEEE Trans. Circuits Syst. Video Technology: Volume 24, Issue 4, Pages 695-703, April 2014

[10] The research paper authored by A. Anees, A. M. Siddiqui, and F. Ahmed, titled "Investigation by Anees, Siddiqui, and Ahmed "Chaotic substitution for highly autocorrelated data in encryption algorithm," Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 9, pp. 3106–3118, Sep. 2014.

[11] L. Liu, Y. Lei, and D. Wang, "Efficient chaotic image encryption scheme with simultaneous permutation-diffusion operation," IEEE Access, vol. 8, pp. 27361–27374, 2020.

[12] M. Khalili and D. Asatryan, "Effects of color spaces on improved discrete wavelet transform-based digital image watermarking using Arnold transform map," IET Signal Process., vol. 7, no. 3, pp. 177–187, May 2013.

[13] The scholarly article authored by L. Zhang, J. Wu, and N. Zhou, titled "Exploration by Zhang, Wu, and Zhou,"Image encryption with discrete fractional cosine transform and chaos," in Proc. 5th Int. Conf. Inf. Assurance Secur., vol. 2, 2009, pp. 61–64.

[14] M. Zhang, X.-J. Tong, J. Liu, Z. Wang, J. Liu, B. Liu, and J. Ma, "Image compression and encryption scheme based on compressive sensing and Fourier transform," IEEE Access, vol. 8, pp. 40838–40849, 2020.

[15] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," IEEE Access, vol. 8, pp. 159732–159744, 2020.

[16] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Confusion and diffusion of image pixels using dynamic substitution based on chaos," IEEE Access, vol. 8, pp. 140876–140895, 2020.

[17] F. Masood, W. Boulila, J. Ahmad, Arshad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "Novel privacy approach of digital aerial images based on Mersenne twister method with DNA genetic encoding and chaos," Remote Sens., vol. 12, no. 11, p. 1893, Jun. 2020.

[18] Z. Hua, Y. Zhou, and H. Huang, "Image encryption based on cosine-transform-based chaotic system," Inf. Sci., vol. 480, pp. 403–419, Apr. 2019.

[19] G. Kaur, R. Agarwal, and V. Patidar, "Multiple order optical transform for 2D image encryption based on chaos," Eng. Sci. Technol., Int. J., vol. 23, no. 5, pp. 998–1014, Oct. 2020.

[20] Abhishek, S. N. George, and P. P. Deepthi, "Image encryption using piecewise linear chaotic maps through compressive sensing," in Proc. IEEE Recent Adv. Intell. Comput. Syst. (RAICS), Dec. 2013, pp. 48–52.

[21] J. S. Khan and J. Ahmad, "Efficient selective image encryption using chaos," Multidimensional Syst. Signal Process., vol. 30, no. 2, pp. 943–961, Apr. 2019.

[22] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov, "Image encryption using finite-precision error," Chaos, Solitons Fractals, vol. 123, pp. 69–78, Jun. 2019.

[23] A. Anees and I. Hussain, "Innovative method for identifying initial values of chaotic maps in cybersecurity," Symmetry, vol. 11, no. 2, p. 140, Jan. 2019.

[24] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," Eur. Phys. J. Plus, vol. 133, no. 8, p. 331, Aug. 2018.

[25] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image Vis. Comput., vol. 24, no. 9, pp. 926–934, Sep. 2006.

[26] A. Shafique, "Construction of substitution box using chaotic map," Eur. Phys. J. Plus, vol. 135, no. 2, pp. 1–13, Feb. 2020.

[27] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "Color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," Entropy, vol. 22, no. 2, p. 158, Jan. 2020.

[28] C. Assia, C. Yazid, and M. Said, "Detection and characterization of strokes in brain MRIs through support vector machine-based segmentation," J. Mech. Med. Biol., vol. 15, no. 5, Oct. 2015, Art. no. 1550076.

[29] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "DNA sequence operation and secure hash algorithm SHA-2 based chaos-based image encryption," Nonlinear Dyn., vol. 83, no. 3, pp. 1123–1136, Feb. 2016.

[30] Y. Li, C. Wang, and H. Chen, "Pixel-level and bit-level permutation-based hyper-chaos image encryption algorithm," Opt. Lasers Eng., vol. 90, pp. 238–246, Mar. 2017