Proceedings of the International Conference on Sustainable Computing and Data Communication Systems (ICSCDS-2023)
DVD Part Number: CFP23AZ5-DVD; ISBN: 978-1-6654-5579-4

Determining the Security Standards of Different Crypto Algorithms

P Surekha[1]
Assistant Professor, Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Telanagana, India
prekha.572@gmail.com

P Nandini[2]
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Telanagana, India
nandinipalakurthi2001@gmail.com

S Shruthi[3]
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Telanagana, India

M Ankitha[4]
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Telanagana, India
ankithamundlapatti123@gmail.com

P Rishitha[5]
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Telanagana, India
rishithareddy4455@gmail.com

P Kalyani Sai Nikitha[6]
Department of CSE
Gokaraju Rangaraju Institute of Engineering and Technology
Telanagana, India
nikithapulavarthi@gmail.com

Abstract*-The protection of digital information has become increasingly important as technology advances. Testing each cryptosystem individually can be time-consuming. To address this problem, we therefore provide technique enabling identifying the most appropriate encryption algorithm for images by using a support vector machine. We have developed an approach to evaluate the security level of encrypted images using a dataset with standardized criteria for encryption cryptography. These parameters, for instance, entropy ,contrast, homogeneity, peak signal-to-noise ratio, mean square error, energy, and correlation serve as features for the dataset, which is categorized into three security levels: tolerable(acceptable), poor(weak), and powerful(strong). ```Our results indicate the effectiveness of our approach in determining the security level of encrypted images.

Keywords: Support Vector Machine (SVM), Security Analysis, Images Encryption, and Cryptosystem.

I. INTRODUCTION

As more multimedia data is transmitted over insecure channels such as the internet, the need for data Security has progressed into major area of research. Researchers have been working on developing new encryption algorithms to protect data from unauthorized access and eavesdropping. Two key elements of image encryption are diffusion and confusion, which were first proposed by Claude Shannon as necessary components of a secure cryptosystem. Both rows and columns, as well as individual pixels, can always be scrambled, although the native pixel intensities are modified by diffusion. However, simply transmitting data in an encrypted format is not enough to guarantee privacy. Weak encryption algorithms can still allow unauthorized users to view the information. The security level of the encryption algorithm used greatly impacts the robustness of the encryption. Using a highly secure encryption method will ensure the integrity, secrecy, and availability of the original image. Because various sorts of information require varying amounts of security, temporal complexity is indeed a crucial aspect to take into account when selecting a cryptographic approach. The kind of software that has to be decrypted will determine whichever cryptosystem is used. This is why we suggest a classifier machine-based level of security detection method for picture cryptographic algorithms (svm).

A. Problem Statement

Several encryption algorithms, including those based on chaos theory and transformations, have indeed been presented recently. However, by evaluating their statistical results, it has been found that some of these algorithms are not secure and do not provide sufficient protection. One way to assess an encryption algorithm's degree of protection is measured through analyzing its security parameters. Traditional methods of doing this typically entail doing each of these evaluations separately., which can be time-consuming. To overcome this, we have developed a machine learning model utilizing SVM, which can help you rapidly choose the right encryption technique.

II.Literature Survey

Several encryption methods have been suggested as ways to secure images before transmission. These methods can be based on chaos theory or transformations such as discrete wavelet transformation, discrete curvelet transformation. However, there are many Several picture security ideas have recently been put forth. Another illustration is a Fourier transition as well as chaos-based picture encryption system that, for extra intricacy, employs three separate chaotic sequences. A novel high resolution encryption method that employs chaotic maps is yet another suggestion., This is able to produce vectors of various orders. Additionally, there is a chaos-based selective image encryption scheme that is fast, although not appropriate for text encryption. These algorithms have shown efficient encryption through statistical analysis, but more analysis is needed to fully assess their security. However, it has been noted that chaos-based

encryption schemes have limitations when implemented on a finite precision computer, which can lead to dynamic degradation and make the encryption less secure. Additionally, these systems depend on initial values, making them vulnerable to being broken by identifying those values. In our previous work, a new image encryption technique was proposed that incorporates a bit-plane extraction method and multiple chaotic systems to enhance the security of the chaos-based cryptosystem [4]. This method's objective was to speed up computation whereas simultaneously enhancing secrecy. Another example is a steganographic technique based on the chaotic logistic map (CLM) introduced in [10]. This method addresses the issue of using a single substitution box (S-box) encryption by incorporating multiple S-boxes, with the choice of a certain S-box determined by random values generated by the CLM. S-boxes are a common component in chaos-based image encryption due to their powerful, nonlinear diffusion capabilities. However, the resilience of the S-box determines how strong various encryption techniques are., making the development of strong S-boxes a critical research area for security professionals. To overcome the issue of weak S-boxes, CLM-based methodology was previously proposed to create new S-box in [6]. The Indicators of this S-box can vary with slight changes the starting integers of the CLM. Encrypting colour images is even more challenging than encrypting grayscale images, as all three colour channels Must be encrypted on (R, G, B). In [7], A visual picture encryption scheme using a composite dynamic map has been developed, using confusion for the encryption of each color component separately, additionally dispersing the confused elements that used a mitochondria Genetic code. Each of the encryption algorithms discussed have varying levels of security, with some being stronger, some being acceptable, and some being weaker, depending on the complexity of their mathematical structure.

C Existing System

Obtaining a dataset that is both well-balanced and highly relevant is challenging in the current system. Even though a large amount of data is available, selecting the appropriate data is difficult. To address this issue, we utilize machine learning tools from the scikit-learn library to extract valuable data.

Limitations: Traditional methods of doing this typically involve making these comparisons one at a time, which can be time-consuming.

III.Proposed System

Several encryption algorithms, including those based on chaos theory and transformations, have just been put out recently. However, by evaluating their statistical results, it has been found that some of these algorithms are not secure and do not provide sufficient protection. Analyzing a cryptography algorithm's security features so is method of determining its level of privacy. To overcome this, we have created a model for machine learning. utilizing SVM, which can assist in quickly selecting an appropriate encryption technique.

A. Approach to proposed System

The actions listed below should be taken to be able to assess security level of a certain algorithm: assemble a sizable collection of data derived from various cypher pictures produced by different cryptographic algorithms.

	Entropy	Energy	Contrast	Correlati	Homoger	MSE	PSNR	Security
0	8	0.01	10.75	-0.5	0.392	222	0.1	Strong
1	7.9999	0.01005	10.745	-0.495	0.3921	221	0.2	Strong
2	7.9998	0.0101	10.74	-0.49	0.3922	220	0.3	Strong
3	7.9997	0.01015	10.735	-0.485	0.3923	219	0.4	Strong
4	7.9996	0.0102	10.73	-0.48	0.3924	218	0.5	Strong
5	7.9995	0.01025	10.725	-0.475	0.3925	217	0.6	Strong
6	7.9994	0.0103	10.72	-0.47	0.3926	216	0.7	Strong
7	7.9993	0.01035	10.715	-0.465	0.3927	215	0.8	Strong
8	7.9992	0.0104	10.71	-0.46	0.3928	214	0.9	Strong
9	7.9991	0.01045	10.705	-0.455	0.3929	213	1	Strong
10	7.999	0.0105	10.7	-0.45	0.393	212	1.1	Strong
11	7.9989	0.01055	10.695	-0.445	0.3931	211	1.2	Strong
12	7.9988	0.0106	10.69	-0.44	0.3932	210	1.3	Strong
13	7.9987	0.01065	10.685	-0.435	0.3933	209	1.4	Strong
14	7.9986	0.0107	10.68	-0.43	0.3934	208	1.5	Strong
15	7.9985	0.01075	10.675	-0.425	0.3935	207	1.6	Strong
16	7.9984	0.0108	10.67	-0.42	0.3936	206	1.7	Strong
17	7.9983	0.01085	10.665	-0.415	0.3937	205	1.8	Strong
18	7.9982	0.0109	10.66	-0.41	0.3938	204	1.9	Strong
19	7.9981	0.01095	10.655	-0.405	0.3939	203	2	Strong
20	7.99	0.01505	10.245	0.0001	0.4021	121	10.2	Acceptable
21	7.9899	0.0151	10.24	0.00011	0.4022	120	10.3	Acceptable
22	7.9898	0.01515	10.235	0.00012	0.4023	119	10.4	Acceptable
23	7.9897	0.0152	10.23	0.00013	0.4024	118	10.5	Acceptable
24	7.9896	0.01525	10.225	0.00014	0.4025	117	10.6	Acceptable
25	7.9895	0.0153	10.22	0.00015	0.4026	116	10.7	Acceptable
26	7.9894	0.01535	10.215	0.00016	0.4027	115	10.8	Acceptable
27	7.9893	0.0154	10.21	0.00017	0.4028	114	10.9	Acceptable
28	7.9892	0.01545	10.205	0.00018	0.4029	113	11	Acceptable
29	7.9891	0.0155	10.2	0.00019	0.403	112	11.1	Acceptable
30	7.989	0.01555	10.195	0.0002	0.4031	111	11.2	Acceptable
31	7.9889	0.0156	10.19	0.00021	0.4032	110	11.3	Acceptable
32	7.9888	0.01565	10.185	0.00022	0.4033	109	11.4	Acceptable
33	7.9887	0.0157	10.18	0.00023	0.4034	108	11.5	Acceptable
34	7.9886	0.01575	10.175	0.00024	0.4035	107	11.6	Acceptable
35	7.9885	0.0158	10.17	0.00025	0.4036	106	11.7	Acceptable
36	7.9884	0.01585	10.165	0.00026	0.4037	105	11.8	Acceptable
37	7.9883	0.0159	10.16	0.00027	0.4038	103	11.9	Acceptable
38	7.9882	0.01595	10.155	0.00028	0.4039	102	12	Acceptable
39	7.9881	0.016	10.15	0.00029	0.404	101	12.1	Acceptable
40	7.9799	0.201	9.74	0.0012	0.4122	20	20.3	Weak
41	7.9798	0.02015	9.735	0.0013	0.4123	19	20.4	Weak
42	7.9797	0.0202	9.73	0.0014	0.4124	18	20.5	Weak
43	7.9796	0.02025	9.725	0.0015	0.4125	17	20.6	Weak
44	7.9795	0.0203	9.72	0.0016	0.4126	16	20.7	Weak
45	7.9794	0.02035	9.715	0.0017	0.4127	15	20.8	Weak
46	7.9793	0.0204	9.71	0.0018	0.4128	14	20.9	Weak
47	7.9792	0.02045	9.705	0.0019	0.4129	13	21	Weak
48	7.9791	0.0205	9.7	0.002	0.413	12	21.1	Weak
49	7.979	0.02055	9.695	0.0021	0.4131	11	21.2	Weak
50	7.9789	0.0206	9.69	0.0022	0.4132	10	21.3	Weak
51	7.9788	0.02065	9.685	0.0023	0.4133	9	21.4	Weak
52	7.9787	0.0207	9.68	0.0024	0.4134	8	21.5	Weak

Fig 1. Sample of dataset

Characteristics that are used are as follows:

1. Contrast
   "Contrast analysis examines the variation in pixel values. A greater difference in pixel values results in higher contrast in the image, which improves security. Lower contrast, on the other hand, indicates minimal differences between original and manipulated pixel values."
2. Entropy
   Entropy analysis measures the level of randomness generated by an encryption algorithm in the encrypted image. Depending upon the number of pixels in the image, various images' stochastic values change. For instance, an 8-bit image will have a maximum entropy value of 8, while a single-bit image (binary image) will have a maximum entropy value of 1. For secure encryption, the value of the entropy for encrypted image should be as nearly the highest value as possible.
3. Energy
   This feature parameter measures the degree to which an image contains information. More information is indicated by higher energy values. Simple images

have higher energy values than encrypted images, as they contain more information.

4. Correlation
It is a crucial metric for determining the security of a cryptosystem. It measures how similar the values of adjacent pixels are. High correlation means that the pixel values are very similar. For example, a plain image with a gradual black-to-white gradient would have high correlation in that area. The plain image typically has many regions of high correlation, making its overall correlation higher than that of an encrypted image.
5. Homogeneity
The grey level occurrence matrix (GLCM) is a table that shows the brightness of pixels. A strong encryption will have smaller homogeneity values. Homogeneity can be calculated using the equation: XaXbP (a, b)1 + |a − b| (7). Homogeneity values are divided into three intervals to indicate strong, acceptable, and weak security. These intervals are: [0.3920 0.4020] for strong security, [0.4021 0.4121] for acceptable security, and [0.4122 0.4418] for weak security.
6. Mean square error and peak signal to noise ratio (MSE) (PSNR).
Any two photos may be used to determine the PSNR value. To find the PSNR value, the MSE value must first be calculated involving the two pictures. A high PSNR value between the original and encrypted images indicates that the encrypted image is very similar to the original. picture and the original are extremely similar. Equation demonstrates that the MSE is inverse to the PSNR. For a strong encryption, the difference in PSNR value between the plain and encrypted images should be high and the error between them should be near the maximum.
For PSNR
[0.1000 10.1000] ⇒ for strong security
[10.2000 10pt20.2000] ⇒ for acceptable security
[20.3000 10pt49.9000] ⇒ for weak security
For MSE
[1 100] ⇒ for weak security
[101 200] ⇒ for acceptable security
[201 400] ⇒ for effective(strong) security

III. METHODOLOGY

A. System architecture

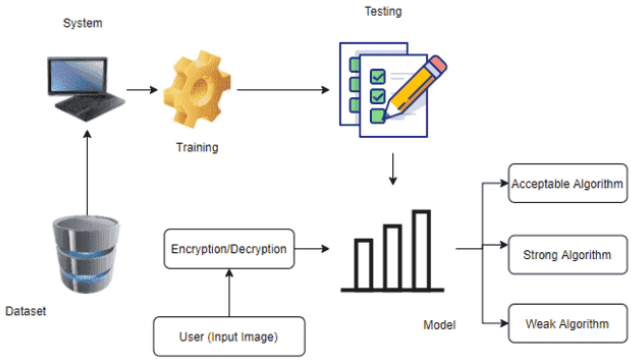

Fig.2 demonstrates the system architecture of the recommended technique.

Algorithms for model implementation

A. A form of classifier called a support-vector model (SVM) is applied to machine learning for regression analyses and classification. They create a model that assigns new examples to one of two categories and employ a hyper - plane or collection of hyper - plane for classification, regression, or even other operations in high- or infinite-dimensional space. The SVM algorithm translates practise examples to spatial positions in order to increase the contrast between the two categories, and new examples are predicted to varies depending on which side of both the divide they fall into a category.

B. DNA computing is a method of Structural biology, biochemistry, and DNA are used in computers instead of conventional silicon-based technology. DNA coding theory uses DNA sequences to represent information and the 4 bases of Dna fragments are expressed using binary integers. There are merely eight different types of sequencing configurations which it adheres to the complementary sequence pairing concept since Dna molecules remain complimentary to one another.

C. C. A quadratic mappings of scaled version known as the logical map is frequently used as an illustration of how basic ou pas dynamical formulas may produce complicated, chaotic behaviour. The map was popularized as a discrete-time demographic model that captures reproduction and starvation effects, but has a pathological problem where Negative population sizes result from certain beginning circumstances and parameter settings.

D. D. The Rubik's Cube Steganographic method takes the Rubik's Cube's permutation idea to secure picture data. Using a key, the Bitwise XOR operator

is used to the image's odd columns and rows. as well as the key is then reversed and applied to the image's even rows and columns. The algorithm has been tested for robustness against several types of attacks and is suitable for applications which require world wide web privacy and streaming.

E. The Lorenz Image Encryption algorithm uses the Lorenz equation, a 3D dynamical system, to encrypt images. The mathematical system's relationship to the basic system components displays chaotic behaviour. and has a much-complicated chaotic behaviour comparison to chaotic 1D or 2D systems. The Lorenz solution is well-known for the "butterfly effect" in scientific investigations and is explored extensively in chaos theory, dynamic system modelling, chaotic controls, and synchronisation phenomena.

IV. RESULTS

Fig 3. User Interface home page

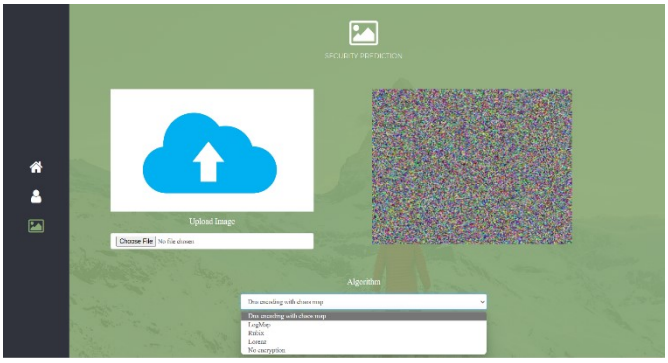

Fig 4. uploading the image and selecting the encryption algorithm

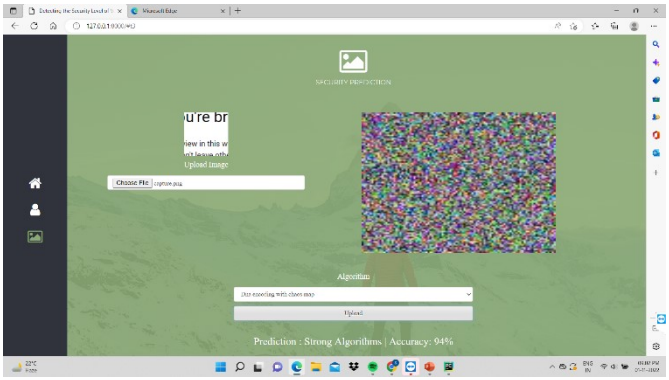

Fig 5. Displaying the results along with encrypted Image

Comparision of existing and proposed model performance

Model	Training Accuracy	Validation Accuracy	Traing Loss	Validation Loss
KNN	88.7	82.6	15.64	35.9
SVM	94	91.1	4.71	49.32

V.CONCLUSION AND FUTURE SCOPE

A Conclusion

In this article, we provide a technique that really can rapidly and precisely assess overall level of safety of different encryption. schemes. Our model is based on a dataset that includes common security parameters of

	precision	recall	f1-score	support
Acceptable	0.88	1.00	0.93	7
Strong	1.00	1.00	1.00	5
Weak	1.00	0.83	0.91	6
accuracy			0.94	18
macro avg	0.96	0.94	0.95	18
weighted avg	0.95	0.94	0.94	18

various encryption schemes as features. We divided the values of these features into three categories: strong, acceptable, and weak, representing different levels of security. We then tested different encryption schemes using our model and found that it can produce correct predictions of security levels at a faster rate than other existing models, with an accuracy of 94%. Additionally, To assess the effectiveness of our suggested paradigm, we ran studies.

B. *Future Scope*

As for future works, studies will look into the application of deep-learning algorithms to determine the level of protection of cryptographic schemes.

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, ‘‘A robust watermarking scheme for online multimedia copyright protection using new chaotic map,’’

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

[4] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, ‘‘A noisy channel tolerant image encryption scheme,’’

[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,”

[6] C. E. Shannon, ‘‘Communication in the presence of noise,”

[7] S. Heron, ‘‘Advanced encryption standard (AES),’’

[8] H. Liu, A. Kadir, and X. Sun, ‘‘Chaos-based fast colour image encryption scheme with true random number keys from environmental noise,’’

[9] Y.-L. Lee and W.-H. Tsai, ‘‘A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations’’

[10] A. Anees, A. M. Siddiqui, and F. Ahmed, ‘‘Chaotic substitution for highly autocorrelated data in encryption algorithm,’’

[11] L. Liu, Y. Lei, and D. Wang, ‘‘A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation’’.,

[12] M. Khalili and D. Asatryan, ‘‘Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map,”

[13] L. Zhang, J. Wu, and N. Zhou, ‘‘Image encryption with discrete fractional cosine transform and chaos,’’

[14] Ramesh, G., Anugu, A., Madhavi, K., Surekha, P. (2021). Automated Identification and Classification of Blur Images, Duplicate Images Using Open CV. In: Luhach, A.K., Jat, D.S., Bin Ghazali, K.H., Gao, XZ., Lingras, P. (eds) Advanced Informatics for Computing Research. ICAICR 2020. Communications in Computer and Information Science, vol 1393. Springer, Singapore. https://doi.org/10.1007/978-981-16-3660-8_52

[15] Dhanke Jyoti Atul et al. (2021) A Machine Learning-Based IoT for Providing an Intrusion Detection System for Security. Microprocessors and Microsystems, Volume 82, 103741. (Elsevier)

[16] Kumar, S.K., Reddy, P.D.K., Ramesh, G., Maddumala, V.R. (2019). Image transformation technique using steganography methods using LWT technique. Traitement du Signal, Vol. 36, No. 3, pp. 233-237. https://doi.org/10.18280/ts.360305

[17] Parameswari, D.V.L., Rao, C.M., Kalyani, D. et al. Mining images of high spatial resolution in agricultural environments. Appl Nanosci (2021).

[18] G. Ramesh et al., “Feature Selection Based Supervised Learning Method for Network Intrusion Detection”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8, Issue-1, May 2019.