ANALYSING THE SECURITY LEVELS OF CRYPTOGRAPHIC ALGORITHMS

by K. NARENDRA KUMAR

ABSTRACT

The development of wireless and mobile communications will lead to data exchange via the Internet. This transmission of data over open public networks is vulnerable to multiple types of attacks. Encryption is the way information can be protected from hackers, so sensitive data can be protected by cryptosystems. With the rise of cyberattacks, encryption has become an important part of modern communication. In the existing proposed encryption algorithms have long been proven to be insecure and pose a serious security risk to sensitive data.

In existing systems, the following algorithms have been proposed: Support Vector Machines (SVM) incorporate an approach to detect the security level of image encryption. The following features extracted from cryptographic images are entropy, contrast, uniformity, peak signal to noise ratio, mean squared error, energy, correlation, and dataset labels are classified into three categories based on security level are: strong, acceptable, and weak to evaluate the performance.

The proposed system uses image encryption algorithms for security level detection such as: Logistic Map, Rubik's Cube Image Encryption, Lorentz Image Encryption, DNA Encoding by binding with Classifiers: XGB Algorithm enables fast algorithm selection and increased encryption security.

CHAPTER 1

INTRODUCTION

1.INTRODUCTION

1.1 Brief Information about the project

Over the past decades, information security professionals and researchers have placed great importance on information security. Encryption was introduced to protect sensitive information from unauthorized access. Encryption is the process of protecting information from unauthorized access. In order to improve the security level of image encryption algorithms, many image encryption algorithms have been proposed so far. In this project we will review different encryption algorithms to find out which one provides better encryption for the image encryption process. Improve the security of information on image communication.

1.2 Motivation for the project

Advancement in fields like artificial intelligence is being used to analyze a student's performance in the following assessments. Many papers have used different algorithms to predict a student's performance, but only a few reports have examined performance trajectories. As a result, tutors could not predict the student's performance in real time. In this system, two models have been used: Regression analysis is implemented in the first set of experiments to estimate students' assessment scores. The model utilized the supervised machine learning method to analyze a student's performance in the assessments. The proposed models help the institutions to predict the performance of a student.

1.3 Objective of the Project

In this system, check the different algorithms to find the security various levels of the encryption algorithms. This system providing the better security in digital communications and improve the security.

1.4 Organization of the Project

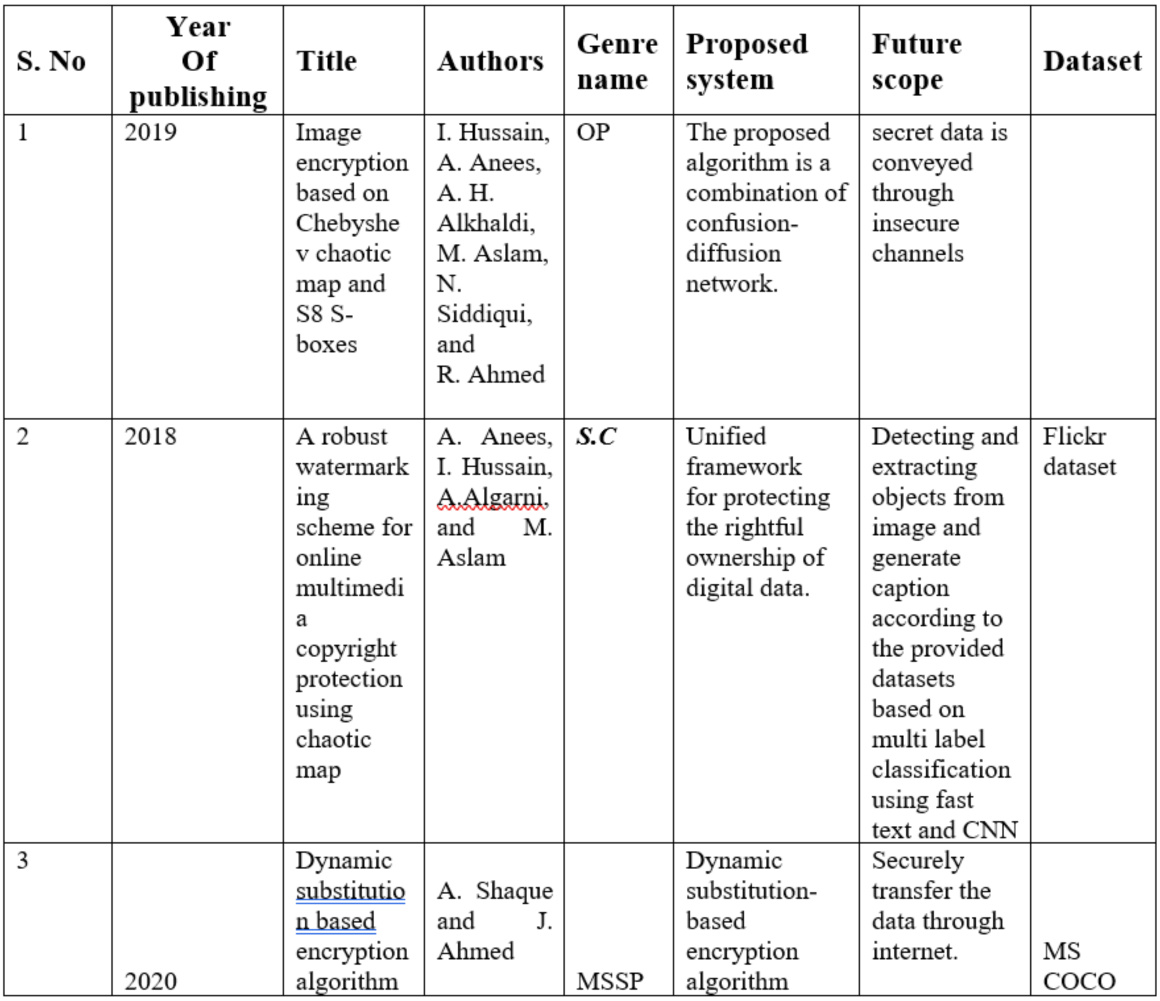
- **Chapter 2: Literature Survey:** This chapter consists of the project's background, possible approaches, introduction, and comparison of technologies.
- **Chapter 3: System Analysis:** This chapter consists of the description of the current system, proposed system, algorithms, and requirement specifications.
- **Chapter 5: System Design:** This chapter mainly consists of modules description and unified modeling language diagrams: use case diagrams, sequence diagrams, collaboration diagrams, and activity diagrams.
- **Chapter 8: Source code:** This chapter mainly consists of sample code for a few modules.
- **Chapter 9: Output Screenshots:** This chapter mainly consists of the output screens of this project.
- **Chapter 10: System Testing:** This chapter mainly consists of testing techniques and module test cases.
- **Chapter 11: Conclusion:** Main conclusion of this project.

CHAPTER 2

LITERATURE REVIEW

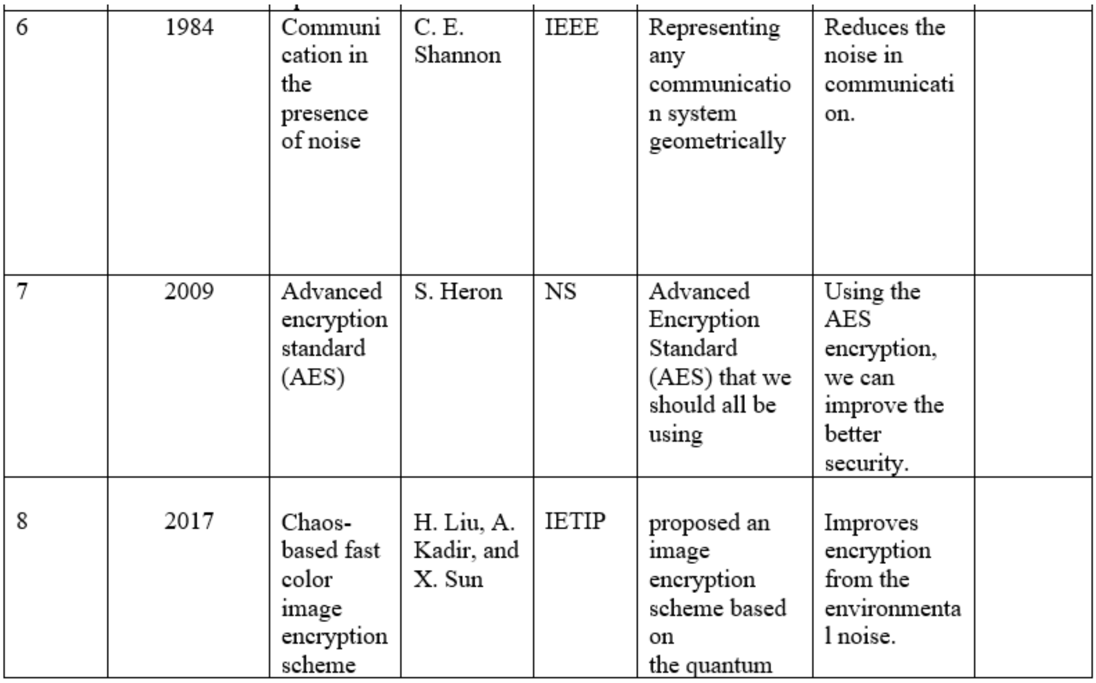
2.LITERATURE REVIEW

The literature review plays a very vital role in the research process. It is a basis from which research thoughts are drawn and developed into concepts and, finally, theories. It also provides the researcher with a bird’s eye view of the research done in that area so far. A researcher will understand where their research stands depending on what is observed in the literature review.



S. No	Year Of publishing	Title	Authors	Genre name	Proposed system	Future scope	Dataset
1	2019	Image encryption based on Chebyshev chaotic map and S8 S-boxes	I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed	OP	The proposed algorithm is a combination of confusion-diffusion network.	secret data is conveyed through insecure channels	
2	2018	A robust watermarking scheme for online multimedia copyright protection using chaotic map	A. Anees, I. Hussain, A.Algarni, and M. Aslam	***S.C***	Unified framework for protecting the rightful ownership of digital data.	Detecting and extracting objects from image and generate caption according to the provided datasets based on multi label classification using fast text and CNN	Flickr dataset
3	2020	Dynamic substitution based encryption algorithm	A. Shaque and J. Ahmed	MSSP	Dynamic substitution-based encryption algorithm	Securely transfer the data through internet.	MS COCO

		for highly correlated data			(DSA)		
4	2014	A noisy channel tolerant image encryption scheme	F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal	WPC	Orthogonal matrices containing columns that form a set of orthonormal basis vectors	Improve the noisy channels through image encryption	
5	2020	A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation	M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet	OLT	Optical image encryption using fractional Fourier transform, DNA sequence operation and chaos theory	Improve the image encryption based on Dna	



6	1984	Communication in the presence of noise	C. E. Shannon	IEEE	Representing any communication system geometrically	Reduces the noise in communication.	
7	2009	Advanced encryption standard (AES)	S. Heron	NS	Advanced Encryption Standard (AES) that we should all be using	Using the AES encryption, we can improve the better security.	
8	2017	Chaos-based fast color image encryption scheme	H. Liu, A. Kadir, and X. Sun	IETIP	proposed an image encryption scheme based on the quantum	Improves encryption from the environmental noise.	

		with true random number keys from environmental noise			logistic map, the scheme is efficient and secure		
9	2014	A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations	Y.-L. Lee and W.-H. Tsai	IEEE	In the proposed method Mosaic image creation, Secret image recovery algorithms are used.	Original secret images can be recovered nearly losslessly from the created mosaic images. Good experimental results have shown the feasibility of the proposed method.	VGG16

Summary of the Literature Survey:

The main goal of all the above papers for the encrypting and decrypting the images to improve the security and check the different algorithms to check the better algorithm for the image encryption. Many articles used different methods, algorithms, and technologies for the image encryption. So as a result, the most appropriate techniques are needed to be used to get result with high accuracy.

CHAPTER 3

SYSTEM ANALYSIS

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

However, several encryption algorithms have been proposed in recent decades Algorithms have proven to be insecure, and as a result, critical data is under great threat. use most However, good encryption algorithms are a very important means of protection against such attacks. Which algorithm is most appropriate in a given situation also depends on the type of data involved secure. However, it may be important to test potential cryptosystems separately to find the best option processing time. To quickly and accurately select the appropriate encryption algorithm.

In existing systems, the following algorithms have been proposed: Support Vector Machines (SVM) incorporate an approach to detect the security level of image encryption. The following features extracted from cryptographic images are entropy, contrast, peak signal to noise ratio, mean squared error, energy, correlation. Dataset labels are classified into three categories based on security level are: strong, acceptable, and weak to evaluate the performance.

3.1.1 DRAWBACKS:

- High Variance
- High Complexity

3.2 PROPOSED SYSTEM

The proposed algorithm uses image encryption algorithms for security level detection such as: Logistic Map, Rubik's Cube Image Encryption, Lorentz Image Encryption, DNA Encoding by Binding with Classifiers: XGB Algorithm enables fast algorithm selection and increased encryption security.

In this system we used different encryption algorithms for better prediction whether it is strong, weak, acceptable. System improves to predict the better algorithms for the image encryption.

3.3.1 ADVANTAGES:

- Better Encryption
- Low Variance

3.4 SYSTEM ARCHITECTURE:

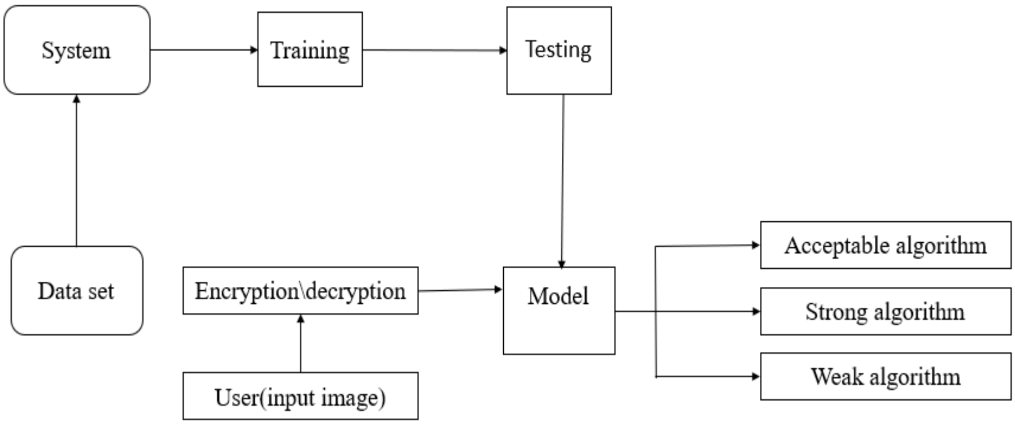


Fig 3.4 System Architecture

.

3.6 MODULES

3.5 SYSTEM:

- **Dataset**

The system takes the dataset uploaded by the user and divides it into two different datasets. One dataset is used for training the data, and the other dataset is used for testing the data.

- **Data Preprocessing**

  The dataset may contain unnecessary values, resulting in wrong predictions or low accuracy. So, after uploading the dataset, it has to be pre-processed so that the unnecessary values will be removed and the prediction will be based on the critical attributes. Therefore, the accuracy will also be higher.

- **Model Training**

  After pre-processing the data, the system should train the dataset using different models to analyze the given data and provide the results to the user based on the inputs. In this system, supervised techniques have been used to predict the performance of a student.

- **Prediction**

  The system takes the input of Plain Image from the user and predicts using the best model among the trained ones.

3.5.1 User:

- **Upload Data:**

  The user uploads a dataset containing Image Features and parameters.

- **View Data:**

  The user views the data in the web app after it is cleaned. The user can also search any record by typing any keyword in the search box.

- **Model Testing:**

  The user can test all possible models the system trains using the testing dataset and view their accuracies.

- **Prediction:**

The user enters the plain image to predict that which algorithm is strong, weak, acceptable.

3.6 PYTHON LIBRARIES

3.6.1: Pandas

- Pandas are very famous libraries in python language.
- They are used mainly for the analysis of data.
- It provides the best performance when we are working with large datasets.
- It also ensures that missing values in the dataset won’t affect the performance or efficiency of the system.
- To work with the pandas' library, one does not require the core knowledge of python language.

3.6.2: Numpy

- Arrays of Numpy offer modern mathematical implementations of massive data. It makes the execution of these projects much more manageable and accessible.
- It is one of the most commonly used libraries in the python programming language.
- It is used mainly for scientific computing in python.
- It can manipulate different shapes according to the user's wish.
- Numpy is primarily used in python language when working with arrays.

3.6.3: Scikit-Learn

- The random module is used for the analysis of the data.
- Everyone can access it with ease.
- Users can reuse it in multiple scenarios.
- Model Selection.
- Pre-processing, including Min-Max Normalization.

CHAPTER 4

SYSTEM REQUIREMENTS AND SPECIFICATIONS

4.SYSTEM REQUIREMENTS AND SPECIFICATIONS

4.1 Functional Requirements:

In software requirement specification’s, functional requirements indicate. The developers build requirements/features that allow users to perform a given task.

- Input : User enters the query in image format
- Output : User gets the answer to the image in text format as a description
- Process: To extract the features from the image and caption it accordingly.

4.2 Non-Functional Requirements:

Non-functional requirements establish quality constraints that are essential to the software firm's success.

- Reliability
- Easy to use
- Processing Time

4.3 Software Requirements:

- Operating System: Windows 10 and above
- Programming Language: Python (3.)
- Frontend: HTML, CSS, Django
- IDE: PyCharm

4.4 Hardware Requirements:

- Processor specification: I5 and above
- RAM: 8GB (MIN)

CHAPTER 5

SYSTEM DESIGN

4. SYSTEM DESIGN

5.1 UML DIAGRAMS:

Unified Modeling Language Diagrams are the complete form of UML diagrams. The primary goal of the UML diagrams is to simplify the model creations for the system. It can be used for different scenarios, such as visualization to construct a model, specify any requirements in the model, etc. It consists of various practices which are successful in object-oriented software engineering. It is one of the essential stages in the process of developing software.

GOALS :

- To provide users with modeling diagrams to express the systems hassle-free.
- Provide extensibility to extend the depth of concepts.
- Be independent, i.e., do not depend on other programming languages.
- To give a basic structure to understand the models easily.
- It supports many high-level development concepts.

5.1.1 DATA FLOW DIAGRAM :

A data flow diagram is also known as DFD. It depicts how a system handles data when the user gives input and desires output. From its name, it is crystal clear how it works. It shows how information passes from one stage to the other stage. The data flow diagram primarily uses modeling. The data flow diagram is one of the basic primary tool modelings. It can be partitioned into different groups, each reflecting an increase in information flow.

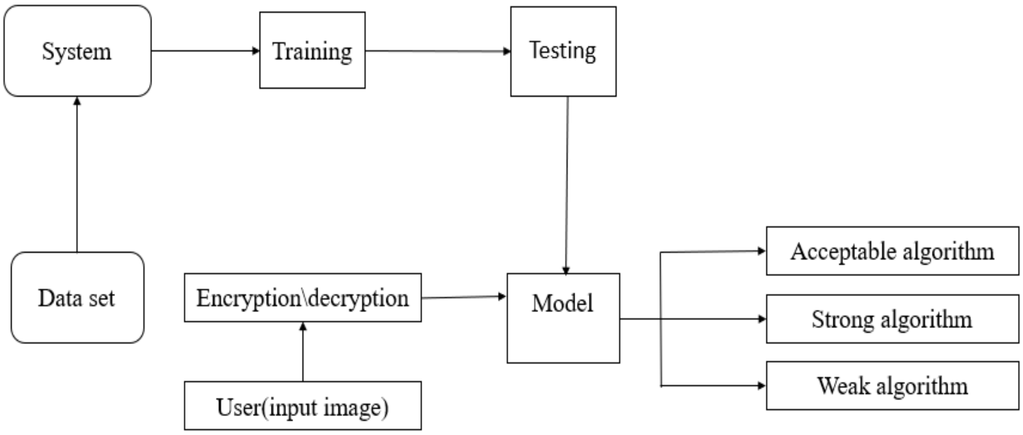


Fig 5.1.1: Data Flow Diagram

5.1.2 SEQUENCE DIAGRAM :

It is a kind of relation diagram representing the relationship between different stages and the order in which they relate. In the chart, the consumer will interact with the application. They are also known by other names, such as occasion diagrams, situations, and timing diagrams.

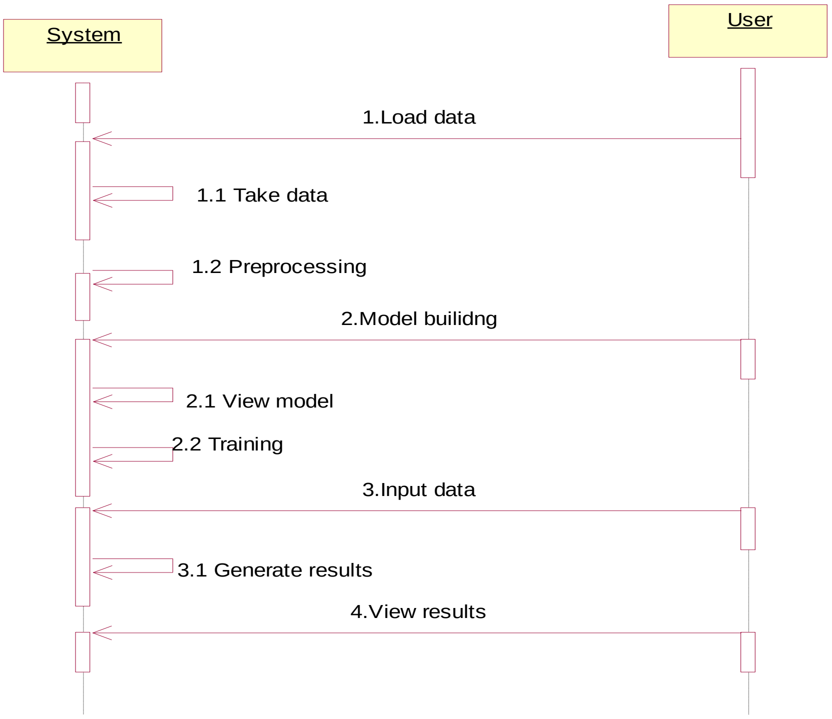


Fig 5.1.2: Sequence Diagram

5.1.3 USE CASE DIAGRAM FOR USER :

Use case diagram is one of the primary modeling tools in UML diagrams. Its primary aim is to provide a graphical representation of what the system does with different use cases respective to actors and goals and their relationship with each other.

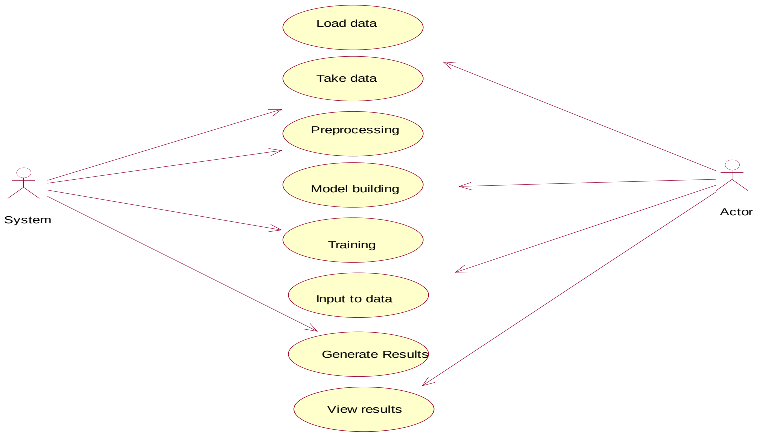


Fig 5.1.3: Use Case Diagram

5.1.4 ACTIVITY DIAGRAM :

The activity diagram describes the activity of the process in step by step process in terms of choices, iterations, and concurrencies. It exhibits the general flow of control in the system. Activity diagrams may be used in the Unified Modeling Language to walk through a system component's business and operational functions.

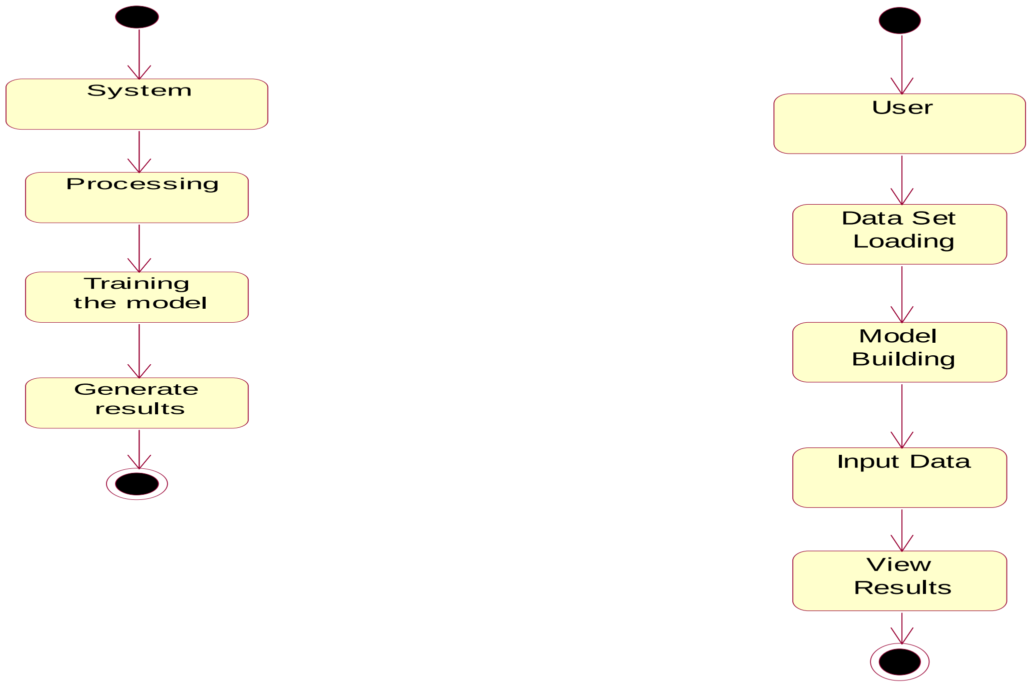
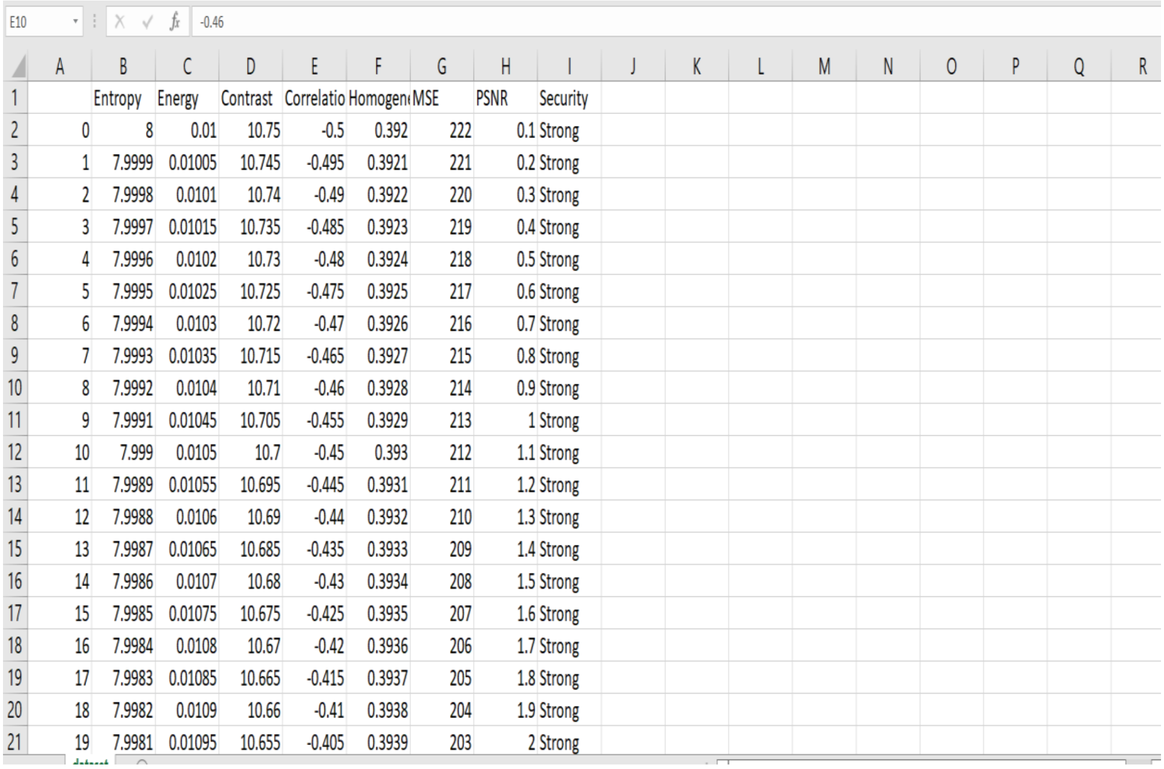


Fig 5.1.5: Activity Diagram

CHAPTER 6

DATASET

5. DATASET



E10 -0.46

	A	B	C	D	E	F	G	H	I
1		Entropy	Energy	Contrast	Correlatio	Homogen	MSE	PSNR	Security
2	0	8	0.01	10.75	-0.5	0.392	222	0.1	Strong
3	1	7.9999	0.01005	10.745	-0.495	0.3921	221	0.2	Strong
4	2	7.9998	0.0101	10.74	-0.49	0.3922	220	0.3	Strong
5	3	7.9997	0.01015	10.735	-0.485	0.3923	219	0.4	Strong
6	4	7.9996	0.0102	10.73	-0.48	0.3924	218	0.5	Strong
7	5	7.9995	0.01025	10.725	-0.475	0.3925	217	0.6	Strong
8	6	7.9994	0.0103	10.72	-0.47	0.3926	216	0.7	Strong
9	7	7.9993	0.01035	10.715	-0.465	0.3927	215	0.8	Strong
10	8	7.9992	0.0104	10.71	-0.46	0.3928	214	0.9	Strong
11	9	7.9991	0.01045	10.705	-0.455	0.3929	213	1	Strong
12	10	7.999	0.0105	10.7	-0.45	0.393	212	1.1	Strong
13	11	7.9989	0.01055	10.695	-0.445	0.3931	211	1.2	Strong
14	12	7.9988	0.0106	10.69	-0.44	0.3932	210	1.3	Strong
15	13	7.9987	0.01065	10.685	-0.435	0.3933	209	1.4	Strong
16	14	7.9986	0.0107	10.68	-0.43	0.3934	208	1.5	Strong
17	15	7.9985	0.01075	10.675	-0.425	0.3935	207	1.6	Strong
18	16	7.9984	0.0108	10.67	-0.42	0.3936	206	1.7	Strong
19	17	7.9983	0.01085	10.665	-0.415	0.3937	205	1.8	Strong
20	18	7.9982	0.0109	10.66	-0.41	0.3938	204	1.9	Strong
21	19	7.9981	0.01095	10.655	-0.405	0.3939	203	2	Strong

Fig: 6.1 Dataset

Dataset Description :

- The dataset contains Image features, which are used to predict their performance in the following assessments.
- The size of the dataset is 62 rows and nine columns.
- Testing data: 70%
- Training data: 30%
- Dataset is collected from the reference of:

  https://www.kaggle.com/datasets/imageencryption/image-details

Entropy : Entropy analysis indicates the amount of randomness a cryptographic algorithm has created in a cryptographic image. The maximum entropy value for different images depends on the number of bits in the image.

Equation :

$$Entropy = \sum_{d=1}^{M} p(s_m) log_2(p(s_m))$$

Energy : This parameter is used to indicate how much information the image contains. Higher energy values indicate more information in the image.

Equation :

$$Energy = \sum_{K=1}^{L} im(x, y)^2$$

Contrast : Contrast analysis shows the difference in pixel values.

Equation :

$$Cont = \sum |x - y|^2 z(x, y)$$

Correlation : Correlation refers to how close pixel values are. A large correlation value indicates that the pixel values are very close together.

Equation:

$$\mu_{ab} = \frac{E[a - E(a)][y - E(b)]}{\sqrt{D(a)}\sqrt{D(b)}}$$

Homogeneity : A gray level occurrence matrix (GLCM) provides a tabular representation of pixel brightness. For strong encryption, the uniformity value should be small.

Equation :

$$\sum_{a}\sum_{b}\frac{P(a,b)}{1+|a-b|}$$

Peak Signal To Noise Ratio (PSNR) And Mean Square Error (MSE):

- PSNR values can be calculated between any two images. Before calculating the PSNR value, we need to calculate the MSE value between the two frames of interest.

  A high PSNR value between two images (original and encrypted) means that the processed image is very close to the original.
- MSE is inversely proportional to the PSNR

PSNR Equation:

$$PSNR = 20log_{10}(\frac{max_{val}}{\sqrt{MSE}})$$

MSE Equation:

$$MSE = \frac{1}{XY}\sum_{a=1}^{X}\sum_{b=1}^{Y}(P_{im}(a,b) - C_{im}(a,b))$$

CHAPTER 7

ALGORITHMS

7. ALGORITHM

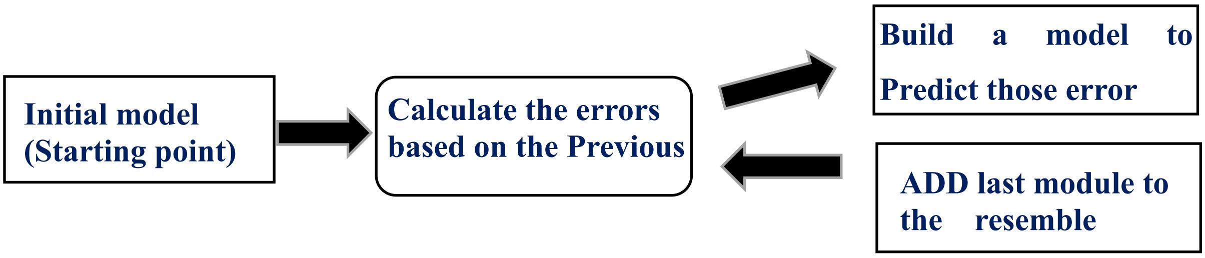
7.1 XG-BOOST ALGORITHM:

It comes under the supervised technique, which can be used for classification and regression problems.

XG – Boost repeatedly builds new models and combine them into an ensemble model.
Initially build the first model and calculate the error for each observation in the data set.
Then you build a new model to predict those residuals(error).
Then you add prediction from this model to the ensemble of models.
XG – Boost is superior compared to gradient boosting algorithm since it offers a good balance between bias and variance gradient boosting only optimized for the variance so tend to overfit training data while XG boost offers regularization terms that can improve model generalization.

Steps involved in random forest algorithm:

- **Step 1:** In XG Boost, Load the libraries e.
- **Step 2:** After loading the libraries load the data set.
- **Step 3:** After loading the data set data cleaning and feature engineering has been done.



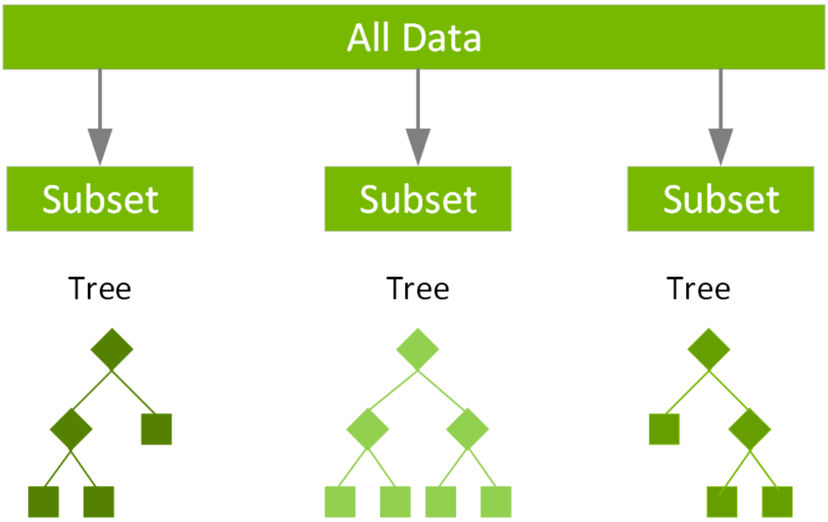


Fig. 7.1.1: R.F. Example

7.2 DNA ENCODING ALGORITHM:

- DNA encoding technique is used for encoding and decoding of images. As we know in medical, DNA sequences have four nucleic acid bases, which are T (thymine), C (cytosine), A (adenine), G (guanine). Here, C and G are complementary, and T and A are complementary to each other.

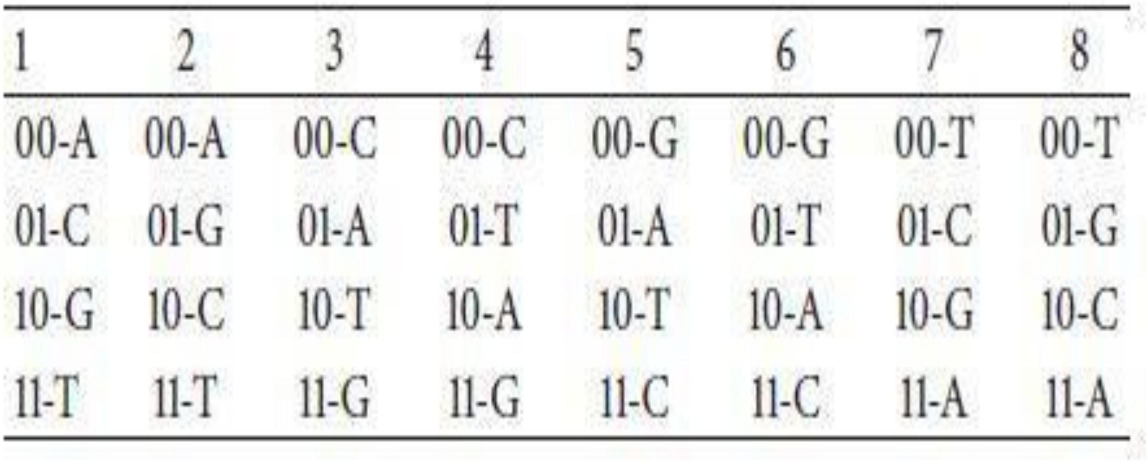
- we come to binary, 1 and 0 are complementary of each other. we are using A, T, C, G denoted as 00,11,01,10 respectively. If we represent 8-bit gray image in a DNA sequence then each pixel will have length of 4.

Steps involved in decision tree algorithm:

- **Step 1:** Resize the input image and convert it into gray scale.
- **Step 2:** Use 32-bit ASCII number as a key to encode the input image. Convert hexadecimal key to 128 bits binary. Selecting any 32 bits and divide them into 4 parts having 8 bit each. Now apply “XOR‟ operation on these bits and convert the answer into decimal.
- **Step 3:** Apply 8 rules of the DNA encoding to convert the input image into DNA encoded image.
- **Step 4:** Take a key image and repeat the same step as above to encode it to get a cipher image.
- **Step 5**: Now that the scrambled image and the encoded input image are DNA encoded, we use a rule to "XOR" both images to get the scrambled DNA encoded image.
- **Step 6**: Now that the output image from step 6 is DNA encoded, we use a rule to convert each pixel to a decimal value to get the final encoded image.

Example:

First pixel of the image is 173, now converting it into binary stream as [10101101], then using the above DNA encoding rule in order to encode obtained stream of bits we will get [GGTC].



1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

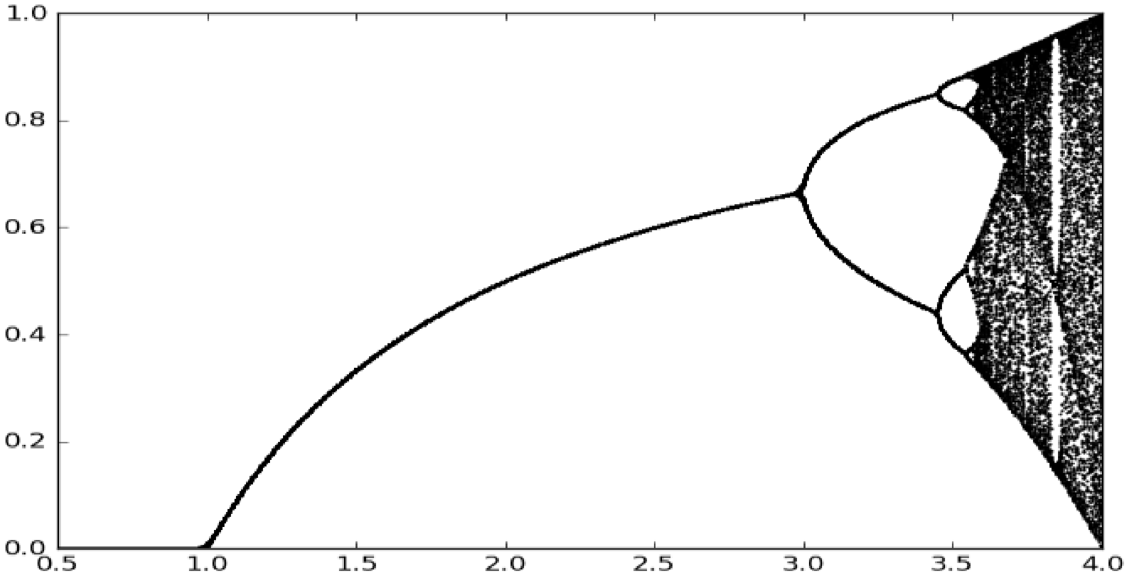
Fig 7.2 DNA Rules

7.2 LOGISTIC MAP ALGORITHM:

- The chaotic theory is the mathematics considering dynamic behavior of the natural and artificial systems which are sensitive to the initial conditions like weather, climate and traffic on road.
- The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. This nonlinear difference equation is intended to capture two effects: reproduction where the population will increase at a rate proportional to the current population when the population size is small.
- starvation (density-dependent mortality) where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment less the current population. However, as a demographic model the logistic map has the pathological problem that some initial conditions and parameter values (for example, if r > 4) lead to negative population sizes. This problem does not appear in the older Ricker model, which also exhibits chaotic dynamics.

Formula:

$$x_n = \mu x_{n-1}(1 - x_{n-1})\ldots\ldots$$



Bifurcation diagram for μ<1

7.4 RUBIK’S CUBE ALGORITHM:

- ➢ This algorithm is based on the principle of Rubik's cube to permute image pixels. To confuse the relationship between original and encrypted images, the XOR operator is applied to odd rows and columns of image using a key. The same key is flipped and applied to even rows and columns of image. Experimental tests have been carried out with detailed numerical analysis which demonstrates the robustness of the proposed algorithm against several types of attacks such as statistical and differential attacks (visual testing).
- ➢ Moreover, performance assessment tests demonstrate that the proposed image encryption algorithm is highly secure. It is also capable of fast encryption/decryption which is suitable for real-time Internet encryption and transmission applications.

Working:

- Generate randomly two vectors KR and KC of length M and N, respectively. Element $KR(i)$ and $KC(j)$ Each take a random value of the set $\mathcal{A}=\{0,1,2\ldots,2\alpha-1\}$. Note that both KR and KC must not have constant values
- Determine the number of iterations, ITERmax, and initialize the counter ITER at 0.

Increment the counter by one: ITER=ITER+1.

- For each row i of image Io,

(a)compute the sum of all elements in the row i, this sum is denoted by $\alpha(i)$

$$\alpha(i) = \sum_{j=1}^{N} \mathrm{I}_o(i,j), \quad i = 1,2,\ldots,M,$$

(b)compute modulo 2 of $\alpha(i)$, denoted by $M\alpha(i)$,

(c) Row i is shifted left or right by $KR(i)$ positions in the circle, as follows (image pixels are shifted left or right by $KR(i)$ positions, where the first pixel is the last pixel):

If $M\alpha(i)$=0⟶right circular shift, else ⟶ left circular shift.

For each column j of image Io,

(a)compute the sum of all elements in the column j, this sum is denoted by $\beta(j)$,

$$\beta(j) = \sum_{i=1}^{M} \mathrm{I}_o(i,j), \quad j = 1,2,\ldots,N,$$

(b)compute modulo 2 of $\beta(j)$, denoted by $M\beta(j)$.

(c)column j is down, or up, circular-shifted by $KC(i)$ positions, according to the following:

If $M\beta(j) = 0 \longrightarrow$ up circular shift

else $\longrightarrow$ down circular shift.

Steps 4 and 5 above will create a scrambled image

(6) Using vector KC, the bitwise XOR operator is applied to each row of scrambled image ISCR using the following expressions:

$$\mathrm{I}_1(2i-1,j) = \mathrm{I}_{\mathrm{SCR}}(2i-1,j) \oplus K_C(j),$$
$$\mathrm{I}_1(2i,j) = \mathrm{I}_{\mathrm{SCR}}(2i,j) \oplus \mathrm{rot}\ 180\left(K_C(j)\right),$$

- where $\oplus$ and rot180(KC) represent the bitwise XOR operator and the flipping of vector KC from left to right, respectively.
- Using vector KR, the bitwise XOR operator is applied to each column of image $I1$ using the following formulas:

$$\mathrm{I}_{\mathrm{ENC}}(i,2j-1) = \mathrm{I}_1(i,2j-1) \oplus K_R(j),$$
$$\mathrm{I}_{\mathrm{ENC}}(i,2j) = \mathrm{I}_1(i,2j) \oplus \mathrm{rot}\ 180\left(K_R(j)\right).$$

- With rot180(KR) indicating the left to right flip of vector KR.
- If ITER = ITER max, then encrypted image IENC is created and encryption process is done; otherwise, the algorithm branches to step 3.

7.5 LORENZ ALGORITHM:

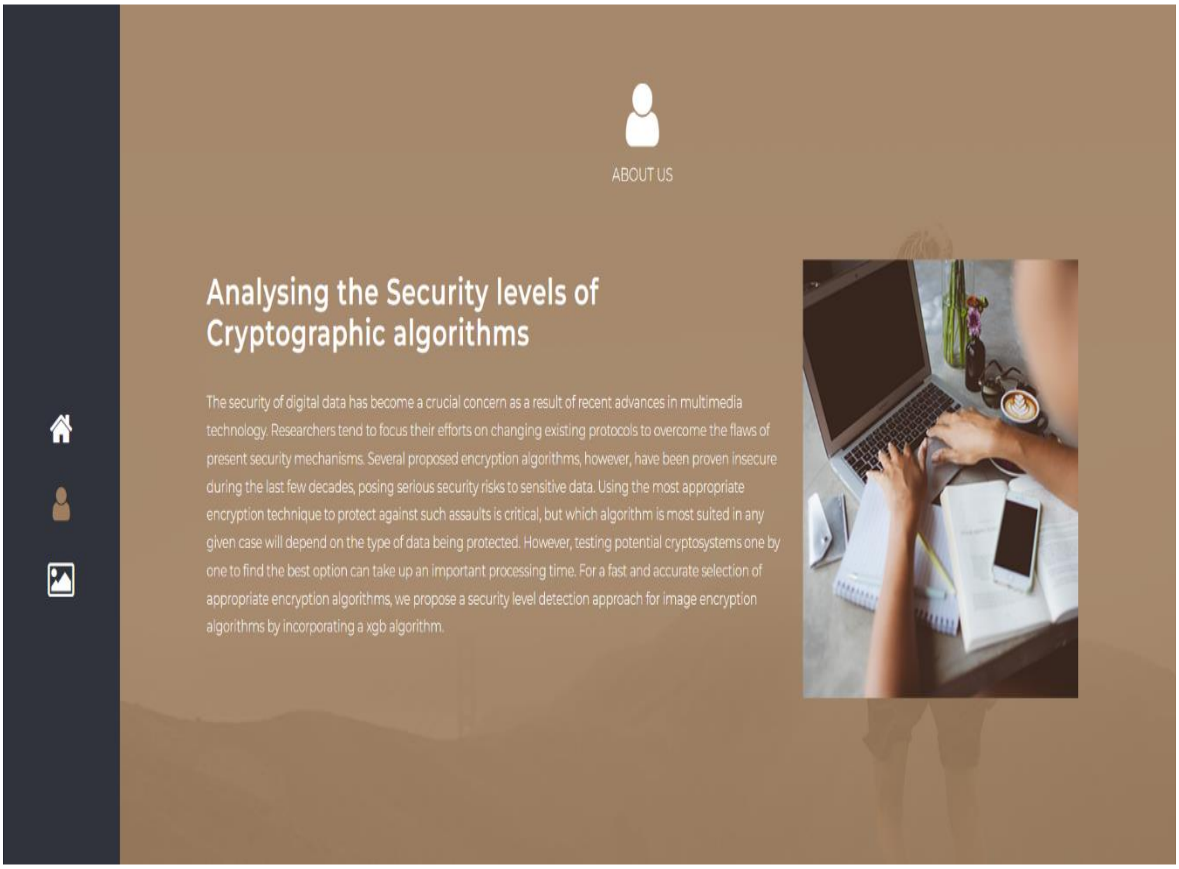
- The Lorenz equation is nothing else than a model of thermally induced fluid convection in the atmosphere. The model was first reported and published by E.N Lorenz in 1963 It is among the classical chaotic systems and implies as the cause of the "butterfly effect" in the scientific studies due to the fact that the attractor has two wings as the butterflies Therefore, it has been widely studied in chaos theory, dynamic system modeling, chaotic control and synchronization phenomenon.
- Lorenz chaotic equation is a 3D dynamical system, which is defined by x, y and z. The equation system gives a chaotic behavior with regard to the initial system parameters. Apart from any 1D or 2D chaotic systems, the Lorenz system has a much-complicated chaotic behavior. By using Lorenz equation, we encrypt the images.

CHAPTER 9
OUTPUT SCREENS

8. OUTPUT SCREENS

ANALYSING THE SECURITY LEVELS OF CRYPTOGRAPHIC ALGORITHMS

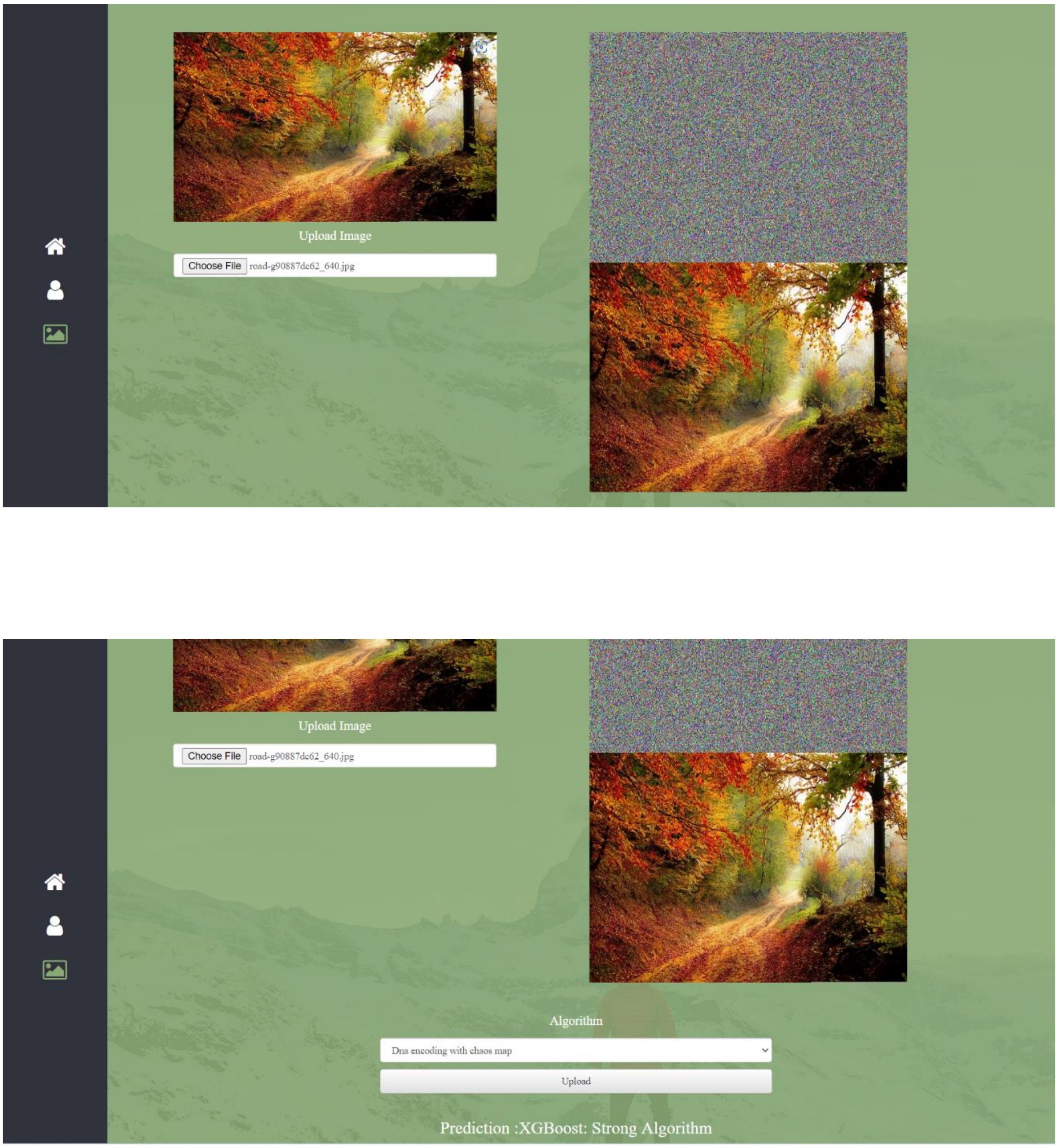
Fig 9.1: Home Page



Analysing the Security levels of Cryptographic algorithms

The security of digital data has become a crucial 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 case will depend on the type of data being protected. However, testing potential cryptosystems one by one to find the best option can take up an important processing time. For a fast and accurate selection of appropriate encryption algorithms, we propose a security level detection approach for image encryption algorithms by incorporating a xgb algorithm.

Fig 9.2: About Page



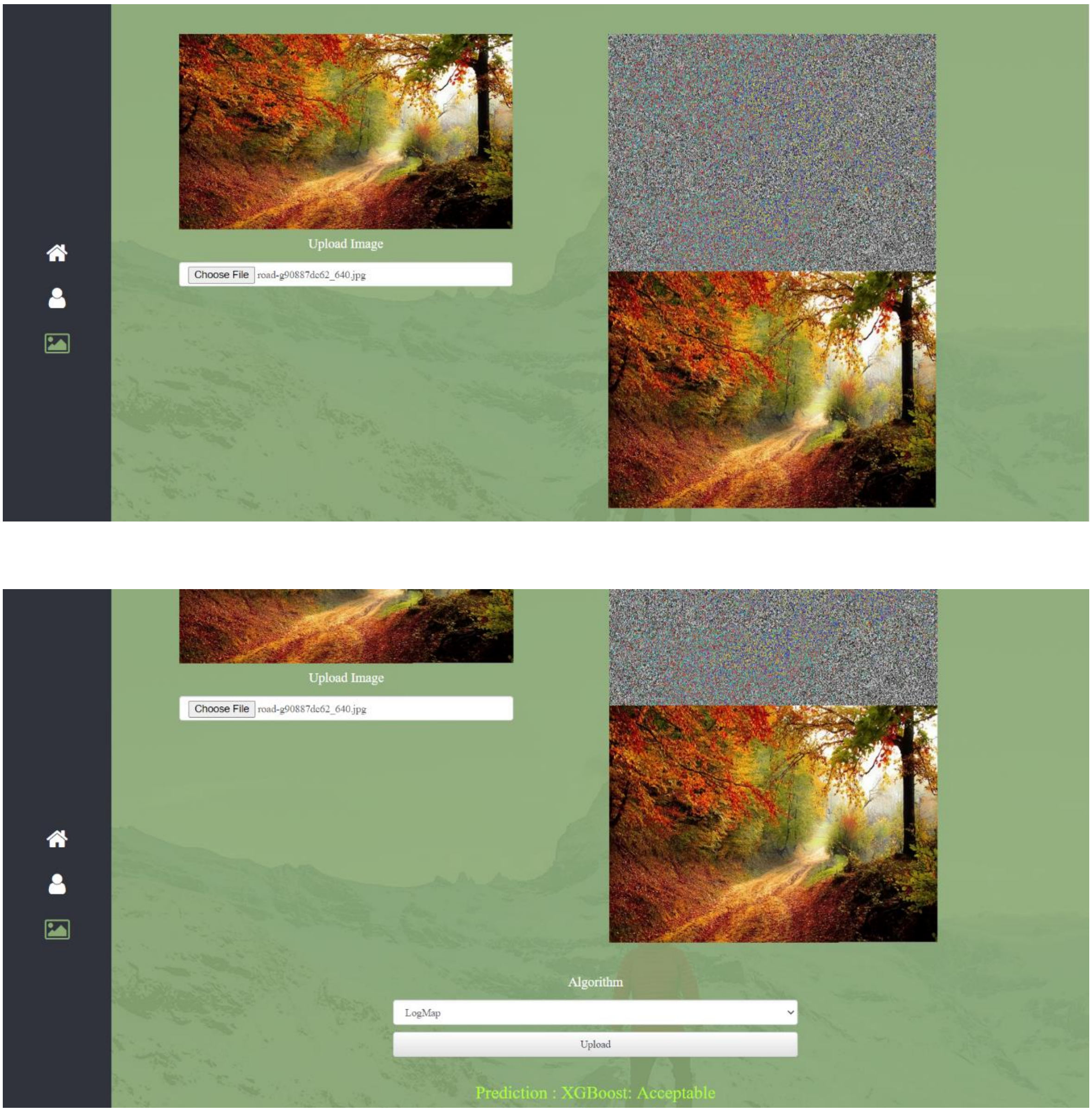
road-g90887dc62_640.jpg

Algorithm

Dna encoding with chaos map

Prediction :XGBoost: Strong Algorithm

Fig 9.3: DNA Encoding Algorithm



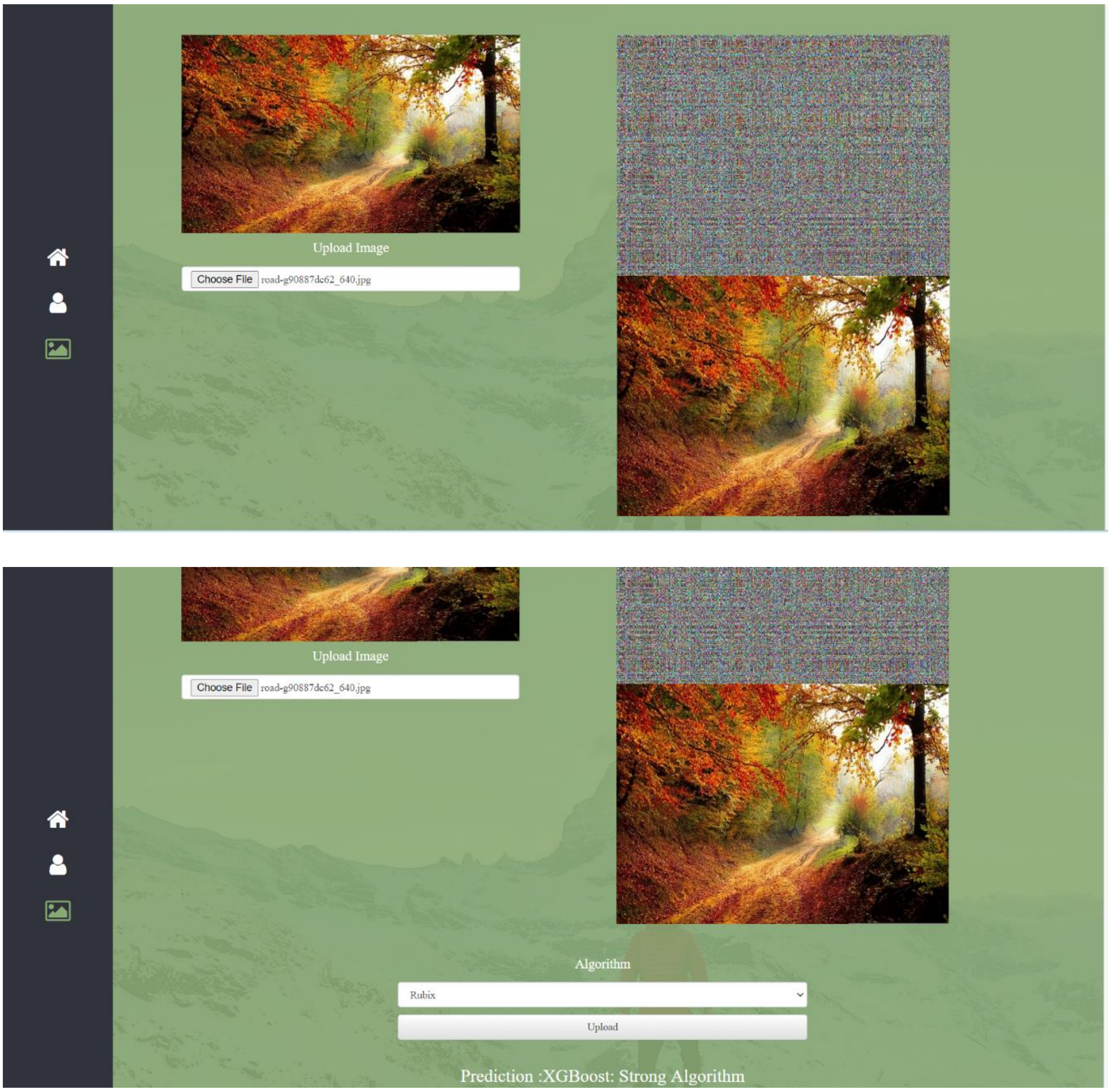
road-g90887dc62_640.jpg

road-g90887dc62_640.jpg

Algorithm: LogMap

Prediction : XGBoost: Acceptable

Fig 9.4: Log map Algorithm



road-g90887dc62_640.jpg

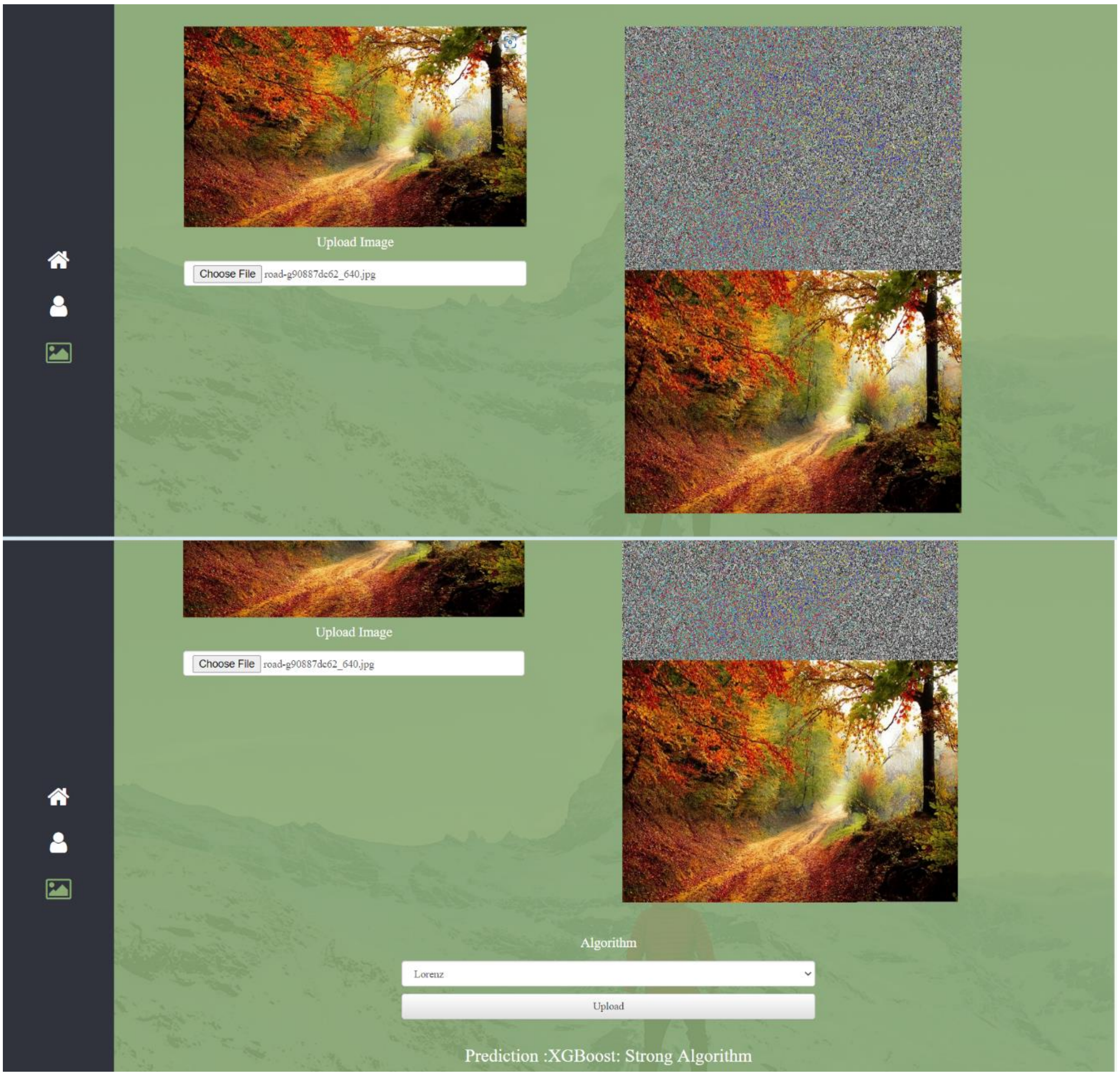
road-g90887dc62_640.jpg

Algorithm

Rubix

Prediction :XGBoost: Strong Algorithm

Fig 9.5: Rubix Algorithm



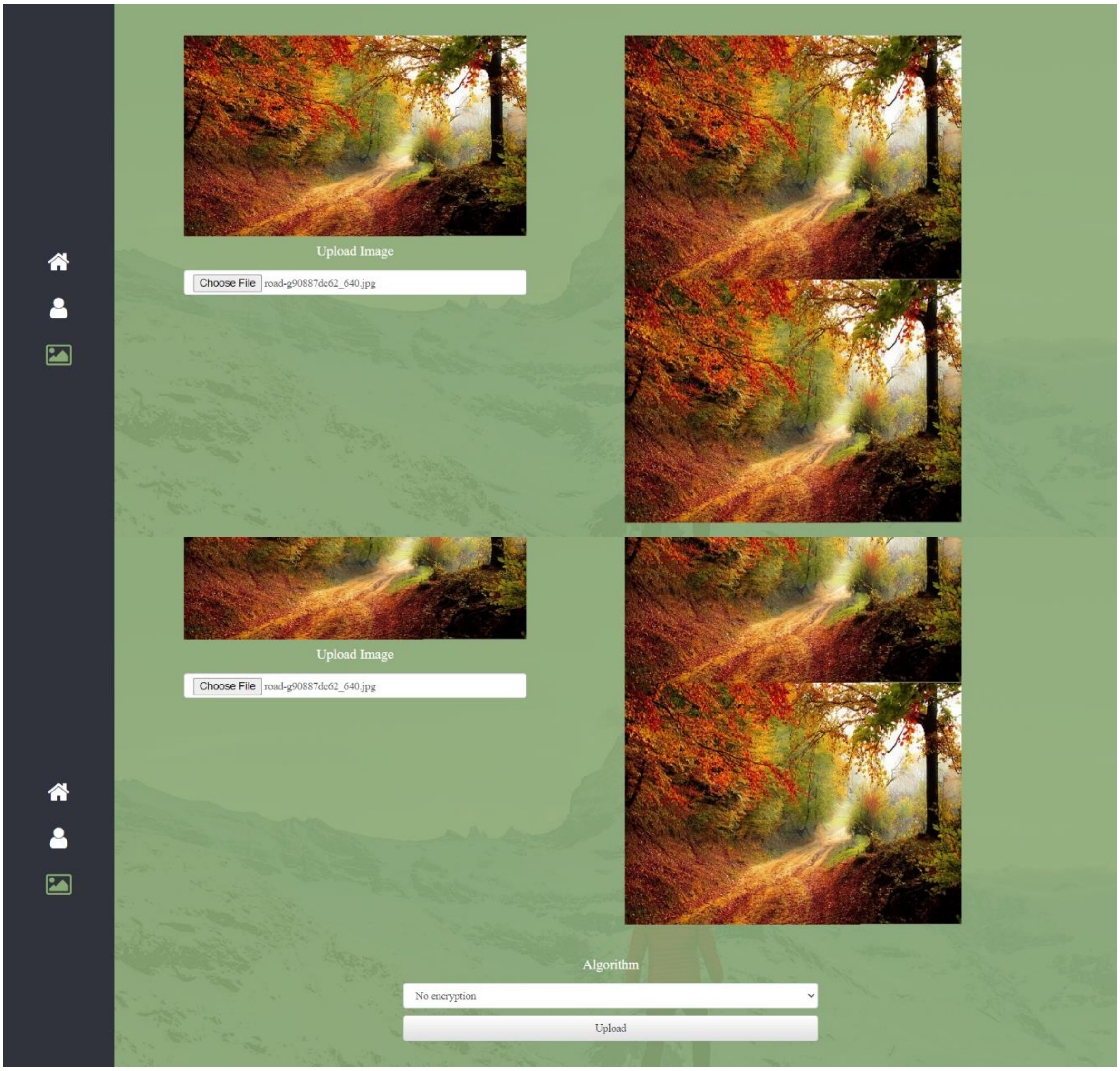
road-g90887dc62_640.jpg

road-g90887dc62_640.jpg

Algorithm: Lorenz

Prediction :XGBoost: Strong Algorithm

Fig 9.6: Lorenz Algorithm



road-g90887dc62_640.jpg

road-g90887dc62_640.jpg

Algorithm: No encryption

Fig 9.7: No Algorithm selected

CHAPTER 10
SYSTEM TESTING

11.TESTING

11.1 Unit Testing:

Unit testing makes sure that every logic and function is working correctly. Because even a minor bug or fault will lead to a crash or failure, it tests all the system parts to make sure everything is working correctly according to its logic. It also runs different tests to ensure that every function in the system configuration is working correctly so the system would not fail at business processes. It ensures that every component is functioning correctly at the primary level. It also provides that every function is working efficiently and accurately.

11.2 System Testing:

System testing tests the blueprint and behavior of the system to verify overall system functionality. This type of testing is done on the whole system to know its quality in terms of business process and also functional requirements. By performing system testing repeatedly, we can improve the quality of a system.

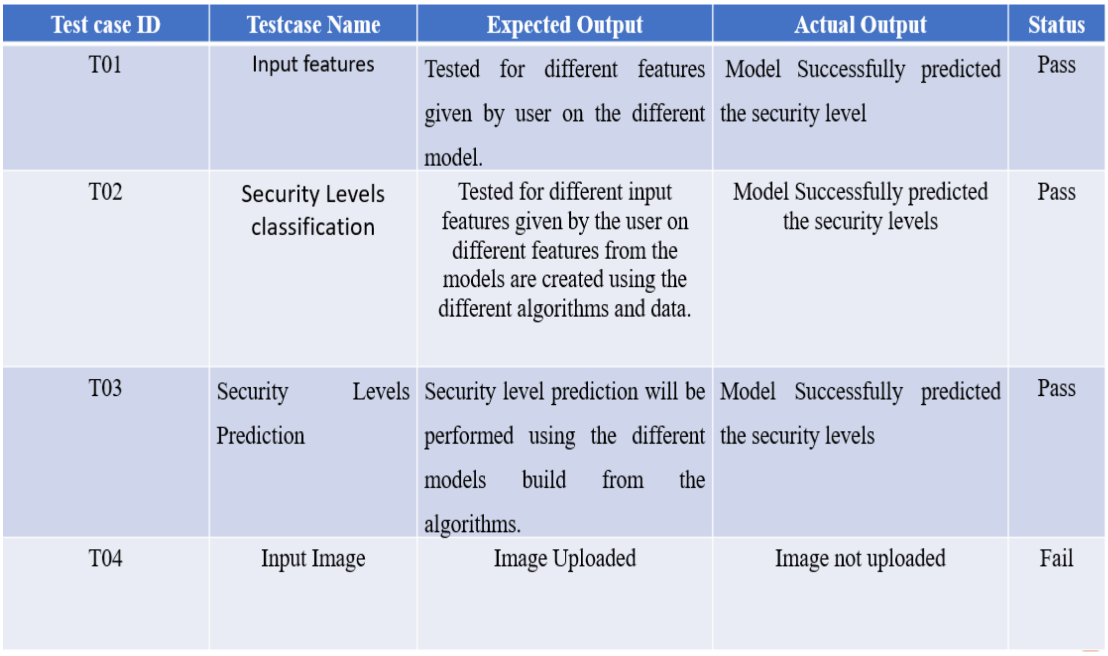
11.3 Integration Testing

This testing checks whether all the functions are working together as a team. The unit testing ensures that every fundamental component of the system is working correctly but does not check whether all those functions are working together. It is significant for the tasks in the program logic to run as a single program to result in the success of a system. This testing also tells us the problems or defects where the system fails to work together as a single unit.

11.4s Functional Testing

It is one of the necessary tests as it ensures all the functions work per the client's requirements or business process. It also gives a better view of system configuration. It should consider the business process per the requirements, which helps satisfy the business process.

TEST CASES



Test case ID	Testcase Name	Expected Output	Actual Output	Status
T01	Input features	Tested for different features given by user on the different model.	Model Successfully predicted the security level	Pass
T02	Security Levels classification	Tested for different input features given by the user on different features from the models are created using the different algorithms and data.	Model Successfully predicted the security levels	Pass
T03	Security Levels Prediction	Security level prediction will be performed using the different models build from the algorithms.	Model Successfully predicted the security levels	Pass
T04	Input Image	Image Uploaded	Image not uploaded	Fail

Table 10.9: Test Cases

CHAPTER 11
CONCLUSION

11. CONCLUSION

Proposed a methodology in the project that can accurately and rapidly detect the security level of various encryption techniques. To generate a dataset describing the resulting security levels, we divided the values of all attributes into three intervals (strong, acceptable, and weak). We then test various encryption methods on the proposed model to see the level of security they offer. Traditional testing methods would take a long time for this process, but the proposed model can perform tests within seconds with an accuracy of 99.

.