International Journal on Applications in Engineering and Technology
Volume 8 : Issue 2 : May 2022, pp 48 – 53 www.aetsjournal.com ISSN (Online) : 2455 - 0523

CRYPTANALYSIS AND IMPROVEMENT OF THE IMAGE ENCRYPTION

DINESH.S[1], DHEENADHAYALAN.R[2], NAGARAJ.R[3], AARTHY.C[4]

[1,2,3] Undergraduate student, Department of computer science and Engineering,
Paavai college of engineering

[4]Assistant Professor, Department of computer science and Engineering,
Paavai college of engineering

Abstract: - This project explains how to develop a chaos-based color picture encryption scheme. For picture encoding, a Feistel network and dynamic Deoxyribonucleic Acid (DNA) encoding system-based image encryption technique is used. Duo confusion and duo diffusion using chaotic maps and attractors were used to achieve the encryption on RGB planes. Confusion and diffusion were performed in two stages in each plane, namely block and plane, using the Logistic Map, Lorenz Attractor, Tent Map, and Lu Attractor with various beginning circumstances and seeds. We have made some essential changes to this encryption system and developed the related chosen-plaintext attack procedure after pointing out and studying these shortcomings. The suggested attack algorithm's efficacy and feasibility were proven through simulated testing and analysis. Finally, improvement recommendations are offered for the flaws in this encryption technique and several contemporary picture encryption systems in order to provide references for future image encryption scheme designers. To encrypt the plain picture, this encryption system uses four encryption steps: Generation of chaotic sequences, Hill encryption, Feistel network, and Pixel diffusion. According to our findings, this encryption scheme's secret key design and encryption method have certain flaws.

Key words: Image encryption, Cryptanalysis, DNA encoding, Feistel Network

1. INTRODUCTION

CYBER SECURITY : Cyber security is a method of safeguarding networks and devices from external attacks. Cyber Security specialists are generally hired by businesses to secure secret information, preserve staff productivity, and boost customer trust in products and services.

The industry standard of confidentiality, integrity, and availability, or CIA, governs the field of cyber security. Only authorized users can access data; only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information; and only authorized users can add, alter, or remove information.

The usage of authentication systems is a key component of Cyber Security. A username, for example, indicates an account that a user wishes to access, but a password is a security technique.

It is nearly hard to prohibit un authorized persons from listening in on any public communication network, such as satellite, mobile phones, and the Internet. For many applications, such as video conferencing, medical imaging, industrial, and military imaging systems, image and video data security has become more crucial. Private multimedia messages exchanged by portable devices over wireless networks and sensitive data transferred in wireless sensor networks are only two examples of applications that need both real-time speed and security. The advanced encryption standard has a set block size (AES).

1.1 IMAGE PROCESSING

A digital image is a two-dimensional image that has been processed by a computer. It refers to the digital processing of

any two-dimensional data in a larger sense. An array of real or complex numbers represented by a finite amount of bits is referred to as a digital picture. An picture on a transparency, slide, photograph, or X-ray is first digitized and stored in computer memory as a matrix of binary numbers. After that, the digital picture can be processed and/or seen on a high-definition television monitor. The picture is stored in a rapid-access buffer memory for display, and the monitor is refreshed at a rate of 25 frames per second to generate a visually continuous display.

1.2 IMAGE PROCESSING FUNDAMENTAL

Digital image processing refers processing of the image in digital form. Modern cameras may directly take the image in digital form but generally images are originated in optical form. They are captured by video cameras and digitalized. The digitalization process includes sampling, quantization. Then these images are processed by the five fundamental processes, at least any one of them, not necessarily all of them.

1.3 IMAGE PROCESSING TECHNIQUES

This section gives various image processing techniques.

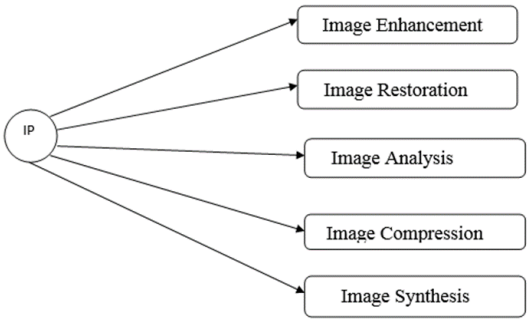


FIG 1.3: IMAGE PROCESSING TECHNIQUES

1.4 IMAGE ENHANCEMENT

Image enhancement operations improve the qualities of an image like improving the image's contrast and brightness characteristics, reducing its noise content, or sharpen the details. This just enhances the image and reveals the same information in more understandable image. It does not add any information to it.

1.5 IMAGE RESTORATION

Image restoration like enhancement improves the qualities of image but all the operations are mainly based on known, measured, or degradations of the original image. Image restorations are used to restore images with problems such as geometric distortion, improper focus, repetitive noise, and camera motion. It is used to correct images for known degradations.

1.6 IMAGE ANALYSIS

Image analysis operations produce numerical or graphical information based on characteristics of the original image. They break into objects and then classify them. They depend on the image statistics. Common operations are extraction and description of scene and image features, automated measurements, and object classification. Image analyze are mainly used in machine vision applications.

1.7 IMAGE COMPRESSION

Image compression and decompression reduce the data content necessary to describe the image. Most of the images contain lot of redundant information, compression removes all the redundancies. Because of the compression the size is reduced, so efficiently stored or transported. The compressed image is decompressed when displayed. Lossless compression preserves the exact data in the original image, but Lossy compression does not represent the original image but provide excellent compression.

1.8 IMAGE SYNTHESIS

Image synthesis operations create images from other images or non-image data. Image synthesis operations generally create images that are either physically impossible or impractical to acquire.

1.9 GRAYSCALE IMAGE

Each pixel is a shade of gray, normally from 0 (black) to 255(white). This range means that each pixel can be represented by eight bits, or exactly one byte. Other grayscale ranges are used, but generally they are a power of 2.

1.10 INDEXED IMAGE

An indexed image consists of an array and a color map matrix. The pixel values in the array are direct indices into a

color map. By convention, this documentation uses the variable name X to refer to the array and map to refer to the color map.

2. MODULE IMPLEMENTATION

2.1 DATA COLLECTION

In this process to collect a data from Kaggle. This Kaggle data collection has an only numerical value and in this data using multiple purpose. Kaggle supports a variety of dataset publication formats, but we strongly encourage dataset publishers to share their data in an accessible, non-proprietary format if possible. Not only are open, accessible data formats better supported on the platform, they are also easier to work with for more people regardless of their tools.

2.2 PREPROCESSING

Data preprocessing is a process of preparing the raw data and making it suitable for a deep learning model. It is the first and crucial step while creating a deep learning model. When creating a machine learning project, it is not always a case that we come across the clean and formatted data. And while doing any operation with data, it is mandatory to clean it and put in a formatted way. So for this, we use data preprocessing task. A real-world data generally contains noises, missing values, and maybe in an unusable format which cannot be directly used for machine learning models. Data preprocessing is required tasks for cleaning the data and making it suitable for a machine learning model which also increases the accuracy and efficiency of a machine learning mode.

2.3 MODEL DEVELOPMENT

The model maintenance plays critical role once the model is deployed into production. The maintenance of machine learning model includes keeping the model up to date and relevant in time tune with the source data changes as there is a risk of model becoming outdated in course of. Also, the configuration management of ML model play an important role in model management as the number of models grow. This article focuses on principles and industry standard practices, including the tools and technologies used for ML model development, deployment, and maintenance in an enterprise environment

2.4 PERFORMANCE EVALUATION

In this process to implement of project Accuracy, recall, Precision, FIS core and ROC curve. Percentage of positive instances out of the total predicted positive instances. Here denominator is the model prediction done as positive from the whole given dataset. Take it as to find out ‘how much the model is right when it says it is right’.

3. MATLAB

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non-interactive language such as C or FORTRAN.

MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran. Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPADsymbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

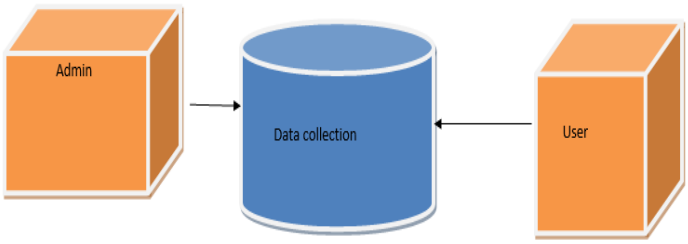
In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises.

MATLAB was first adopted by researchers and practitioners in control engineering, Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of linear algebra and numerical analysis, and is popular amongst scientists involved in image processing. The MATLAB application is built around the MATLAB language.

The simplest way to execute MATLAB code is to type it in the Command Window, which is one of the elements of the MATLAB Desktop. When code is entered in the Command Window, MATLAB can be used as an interactive mathematical shell. Sequences of commands can be saved in a text file, typically using the MATLAB Editor, as a script or encapsulated into a function, extending the commands available. MATLAB provides a number of features for documenting and sharing your work. You can integrate your MATLAB code with other languages and applications, and distribute your MATLAB algorithms and applications.

3.1 INTERFACING WITH OTHER LANGUAGES

MATLAB can call functions and subroutines written in the C



programming language or FORTRAN. A wrapper function is created allowing MATLAB data types to be passed and returned. The dynamically loadable object files created by compiling such functions are termed "MEX-files" (for **M**ATLAB **ex**ecutable).

Libraries written in Java, ActiveX or .NET can be directly called from MATLAB and many MATLAB libraries (for example XML or SQL support) are implemented as wrappers around Java or ActiveX libraries. Calling MATLAB from Java is more complicated, but can be done with MATLAB extension, which is sold separately by Math Works, or using an undocumented mechanism called JMI (Java-to-Mat lab Interface), which should not be confused with the unrelated Java that is also called JMI. As alternatives to the MuPAD based Symbolic Math Toolbox available from Math Works, MATLAB can be connected to Maple or Mathematical. Libraries also exist to import and export MathML.

4. FUNCTIONAL TEST

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

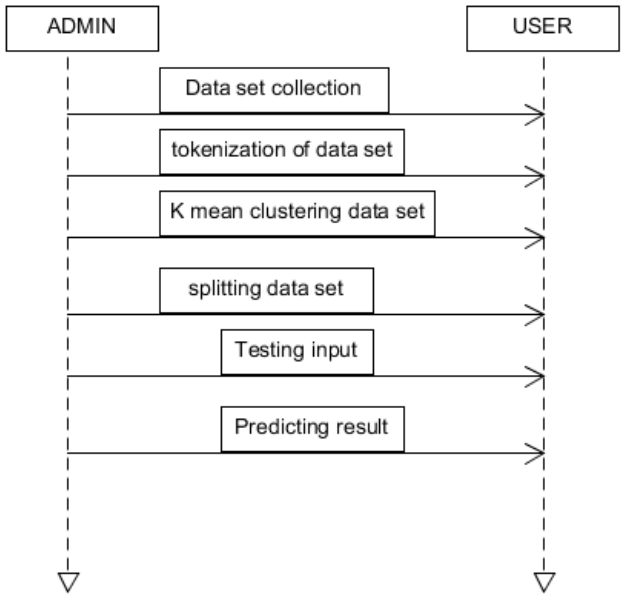
Output : identified classes of application outputs must be exercised.

Systems : interfacing systems or procedures must be invoked.

4.1 BLACK BOX TESTING

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

5. SEQUENCE DIAGRAM



A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct

of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

6. GOALS

The Primary goals in the design of the UML are as follows:

- Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modeling language.
- Encourage the growth of OO tools market.
- Support higher level development concepts such as collaborations, frameworks, patterns and components.
- Integrate best practices.

7. CONCLUSION

In this paper, a newly proposed image encryption scheme based on Feistel network and dynamic DNA encoding, namely IES-FD, is briefly introduced. Then, some security, feasibility and practicability problems in IES-FD are pointed out. After analyzing and discussing these problems, we made necessary improvements to IES-FD and proposed a targeted chosen-plaintext attack algorithm. The proposed attack algorithm first eliminates the pixel diffusion effect of IES-FD through simple processing, and then determines its equivalent substitution matrix, equivalent scrambling matrix, and Hill encryption matrices through about 256 + (M × N/2) special plain images and their corresponding cipher images.

REFERENCE

[1]. X. Zhang, Z. Zhou, and Y. Nia, ‘‘An image encryption method based on the Feistel network and dynamic DNA encoding,’’ IEEE Photon. J., vol. 10, no. 4, pp. 1–14, Aug. 2018.

[2]. H. M. Ghadirli, A. Nodehi, and R. Enayatifar, ‘‘An overview of encryption algorithms in color images,’’ Signal Process., vol. 164, pp. 163–185, Nov. 2019.

[3]. C. Li, Y. Zhang, and E. Y. Xie, ‘‘When an attacker meets a cipherimage in 2018: A year in review,’’ J. Inf. Secur. Appl., vol. 48, Oct. 2019, Art. no. 102361.

[4]. F. Özkaynak, ‘‘Brief review on application of nonlinear dynamics in image encryption,’’ Nonlinear Dyn., vol. 92, no. 2, pp. 305–313, Apr. 2018.

[5]. Y. Zhang, Q. He, Y. Xiang, L. Y. Zhang, B. Liu, J. Chen, and Y. Xie, ‘‘Low-cost and confidentiality- preserving data acquisition for internet of multimedia things,’’ IEEE Internet Things J., vol. 5, no. 5, pp. 3442–3451, Oct. 2018.

[6]. J. Wang, K. Han, S. Fan, Y. Zhang, H. Tan, G. Jeon, Y. Pang, and J. Lin, ‘‘A logistic mapping-based encryption scheme for wireless body area networks,’’ Future Gener. Comput. Syst., vol. 110, pp. 57–67, Sep. 2020.

[7]. Y. Zhang, P. Wang, L. Fang, X. He, H. Han, and B. Chen, ‘‘Secure transmission of compressed sampling data using edge clouds,’’ IEEE Trans. Ind. Informat., vol. 16, no. 10, pp. 6641–6651, Oct. 2020.

[8]. Y. Zhang, Q. He, G. Chen, X. Zhang, and Y. Xiang, ‘‘A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT,’’ IEEE Trans. Ind. Informat., vol. 16, no. 12, pp. 7566–7578, Dec. 2020.

[9]. Y. Zhang, P. Wang, H. Huang, Y. Zhu, D. Xiao, and Y. Xiang, ‘‘Privacyassured FogCS: Chaotic compressive sensing for secure industrial big image data processing in fog computing,’’ IEEE Trans. Ind. Informat., vol. 17, no. 5, pp. 3401–3411, May 2021.

[10]. R. Zhao, Y. Zhang, X. Xiao, X. Ye, and R. Lan, ‘‘TPE2: Three-pixel exact thumbnail-preserving image encryption,’’ Signal Process., vol. 183, Jun. 2021, Art. no. 108019.

[11]. Y. Zhang, R. Zhao, X. Xiao, R. Lan, Z. Liu, and X. Zhang, ‘‘HFTPE: High-fidelity thumbnail-preserving encryption,’’ IEEE Trans. Circuits Syst. Video Technol., early access, Apr. 1, 2021, doi: 10.1109/ TCSVT.2021.3070348.

[12]. A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, and A. M. Iliyasu, ‘‘Efficient chaos-based substitution-box and its application to image encryption,’’ Electronics, vol. 10, no. 12, p. 1392, Jun. 2021.

BIOGRAPHIES

DINESH S is an Undergraduate student, department of computer science and engineering in paavai college of engineering.

DHEENADHAYALAN R is an Undergraduate student, department of computer science and engineering in paavai college of engineering.

ISSN (Online) : 2455 - 0523

NAGARAJ R is an Undergraduate student, department of computer science and engineering in paavai college of engineering.

AARTHY C is an Assistant Professor, department of Computer Science and Engineering in Paavai College of Engineering.