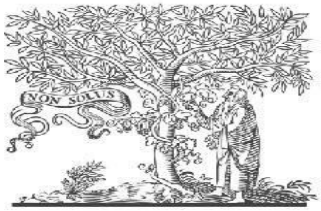
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/94

Title COMPARATIVE STUDY OF IMAGE ENCRYPTION ALGORITHMS USING DATA ANALYSIS

Volume 12, ISSUE 04, Pages: 769-775

Paper Authors

R. Sudha Kishore, J. Divya Sri, A. Hari Sri Veni, G. Mounika, K. Sonia

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Comparative Study of Image Encryption Algorithms Using Data Analysis

R. Sudha Kishore[1], M. Tech(PhD), Associate Professor, Department of CSE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

J. Divya Sri[2], **A. Hari Sri Veni**[3], **G. Mounika**[4], **K. Sonia**[5]
UG Students, Department of CSE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1] sudhakishore@vvit.net, divyasrijonnadula@gmail.com[2], hari.amulothu@gmail.com[3]
guntimounika2407@gmail.com[4] , soniyakamanuri@gmail.com[5]

Abstract

The aim of the application is to facilitate secure transmission of images by performing a comparative analysis of different image encryption algorithms. This project involves examining and comparing algorithms such as DES, Triple DES, AES, RSA, and BLOWFISH. In today's digital world, maintaining high levels of security is essential for nearly all digital services, including communication over the internet, military and medical imaging systems, and multimedia systems. Digital photographs containing important information must be stored and transmitted with a certain level of security. To accomplish this, data is analyzed using a descriptive model that takes into account key variables such as block size, rounds, memory, key size, and the year the algorithm was developed. The outcome of this project is a tool that can help users differentiate between secure algorithms and select the best algorithm for their specific needs.

Keywords: Encryption, Decryption, RSA, AES, Triple DES, IDEA, Blow fish.

Introduction

Due to the rapid increase in digital image information exchange, it is now crucial to prioritize security for safe transmission. To ensure secure transmission over the internet, the encryption of images plays a vital-role. This process involves converting a plain image into an encrypted image using a secret key. Additionally, there is a high demand for the analysis of various image encryption algorithms to protect images from potential attacks.Currently, there is no comprehensive system that provides a detailed overview of various algorithms, making it challenging for users to distinguish and select the suitable one according to their requirements. Proper algorithm selection is crucial in enhancing application security.To address this issue, our project involves a comparison of different image encryption algorithms, including DES, Triple DES, AES, RSA, and BLOWFISH. We conduct an analysis based on specific key factors, enabling clients to determine the most appropriate algorithm that aligns with their needs.

Literature Survey

As part of our project, we conducted a review of ten recent journal papers related

to our topic. One of these papers focused on comparing encryption algorithms using two metrics: computing time and memory usage. The authors discovered that the RSA algorithm had the longest computing time, making it the slowest, while the Blowfish algorithm was the fastest, followed by AES and 3DES. The DES algorithm, however, had poor performance compared to other algorithms, and therefore has lower security. Another paper conducted a comparative analysis of three algorithms, which we extended in our project by comparing all five algorithms and determining the best one based on specific key factors aligned with client requirements. Furthermore, one of the journal papers proposed an improved version of the AES encryption algorithm to establish a secure and symmetric image cryptography technique. In a bid to address the challenge of textured regions prevalent in other cryptographic techniques, the AES encryption algorithm has been improved to incorporate a bit stream generator for image cryptography. Detailed reports were presented on the outcomes of the analysis and implementation. Another research paper reviewed several cryptographic algorithms employed in image encryption, with a particular focus on AES and DES encryption algorithms. The authors highlighted the strengths and weaknesses of each algorithm, assessing the time taken and the key types utilized in these encryption techniques. Furthermore, they analysed which algorithm required more processing.

Problem Identification

A range of cryptographic methods is available, and the choice of which to use depends on the specific demands of the application, such as the desired level of confidentiality and the number of rounds required. It is important to note that each cryptographic algorithm has its own unique strengths and limitations. In order to effectively utilize image encryption, it is essential to determine the optimal algorithm that meets the user's needs. This process can be highly beneficial in helping the end user select an appropriate encryption method.

Methodology

Image encryption is the process of utilizing an encryption algorithm to encode a confidential image, thereby preventing unauthorized access by individuals. Cryptography is composed of two primary elements: plain text and cipher text. Plain text refers to the information intended for the recipient, while cipher text is the encrypted version of the plain text. Encryption and decryption algorithms are categorized into two types: symmetric and asymmetric key encryption. Our project involves an analysis of five distinct algorithms, namely RSA, AES, Triple DES, DES, and Blowfish. RSA utilizes two keys, one public and one private, for encryption and decryption and is an Asymmetric Key Encryption algorithm. Conversely, AES, Triple DES, DES, and Blowfish are Symmetric Key Encryption algorithms,

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

utilizing one key for both encryption and decryption.

1. RSA Algorithm

The RSA algorithm belongs to the asymmetric key algorithm family, which entails the use of distinct keys for encryption and decryption by the sender and recipient. In RSA, the encryption strength is determined by the size of the key, allowing us to double or triple the key size based on our requirements. Consequently, the key size can vary between 1024 and 2048.

1. Select two largest prime numbers p and q
2. Calculate n=pxq
3. Calculate $\phi(n)=(p-1)x(q-1)$
4. Select an integer 'e', such that gcd(e, $\phi(n)=1$ where $1<e<\phi(n)$ and make as public key or encryption key
5. Calculate d using $d=e-1 \bmod \phi(n)$ d is private key or decryption key

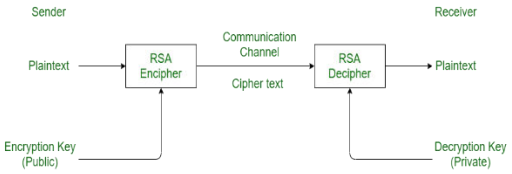


Fig 1. RSA algorithm

2. DES Algorithm

The Symmetric Key block cipher known as the Data Encryption Standard (DES) utilizes a Feistel Cipher implementation. Its structure consists of 16 rounds, with a block size of 64 bits and a key length of 64 bits. However, it's important to note that only 56 out of the 64 key bits are used in the encryption algorithm, resulting in an effective key length of 56bits.

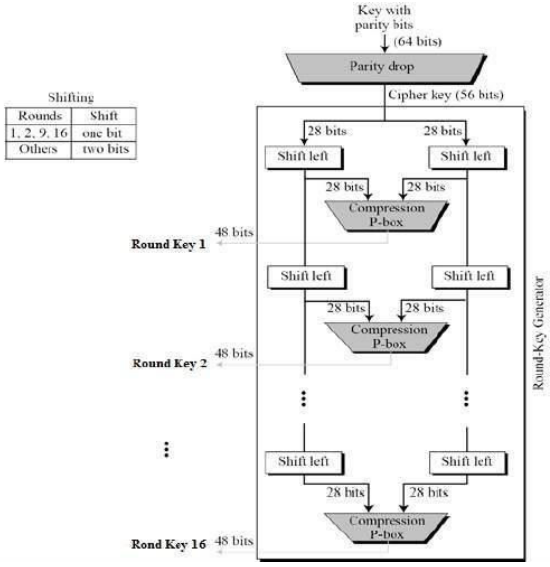


Fig 2. DES algorithm

3. AES Algorithm

Unlike the Feistel cipher, AES is an iterative cipher. In AES, a plaintext block of 128 bits is represented as 16 bytes and arranged in a matrix of four rows and four columns. The number of rounds used in AES varies according to the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round in AES employs a 128-bit round key derived from the original AES key, and this key is unique to each round.

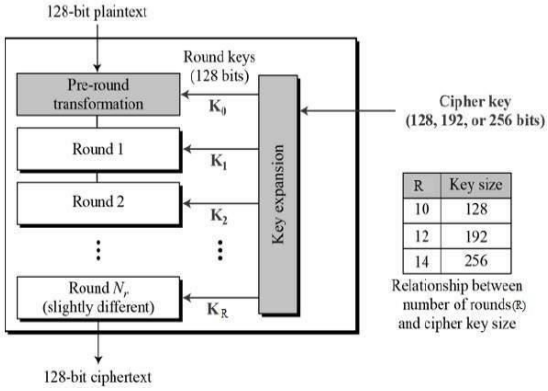


Fig 3. AES algorithm

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

4. Triple DES Algorithm

Triple DES is an encryption method that utilizes different key selection techniques. The first technique involves using three distinct keys, while the second technique involves using two identical keys and one different key. The third technique, on the other hand, employs three identical keys.

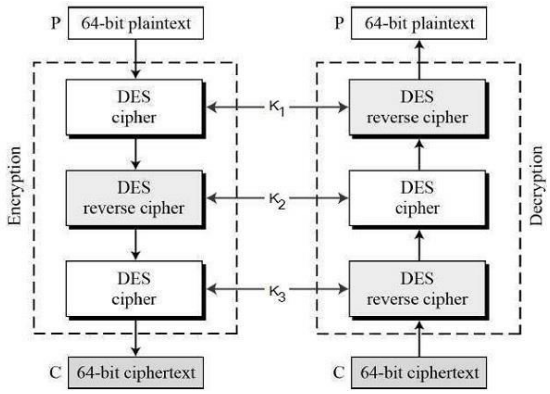


Fig 4. Triple DES Algorithm

5. BLOWFISH Algorithm

Blowfish is a symmetric block cipher with a variable-length key that ranges from 32 to 448 bits and a block size of 64 bits. It is a viable alternative to DES and IDEA encryption algorithms due to its superior speed and free availability. Blowfish utilizes 16 Feistel-like iterations, where each iteration operates on a 64-bit block consisting of two 32-bit words.

During the encryption process, a 32- to 448-bit key is used to generate 18 32-bit sub keys and four 8x32 s-boxes containing 1024 entries. Each s-box element has a size of 32 bits, and the keys are stored in a k-array while the sub keys are stored in a P-array. There are four s-boxes, each containing 256 32-bit entries.

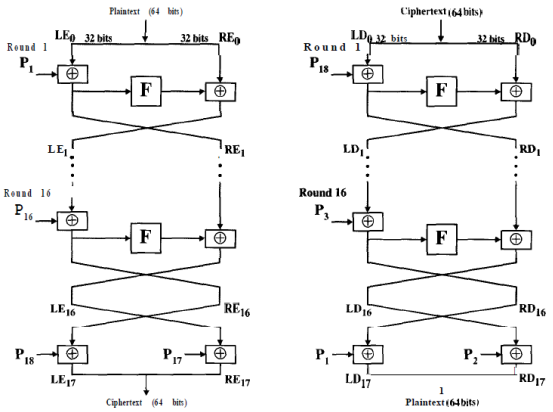


Fig 5. BLOWFISH Algorithm

5. Data Analysis

In today's era, an immense amount of information is being generated, which is commonly referred to as Big data. Data analysis involves the process of refining, modifying, and transforming raw data into meaningful insights that enable businesses to make well-informed decisions. These insights are then presented in the form of charts, tables, images, and graphs, collectively called Data Visualization.

Our project involves a descriptive model analysis of encryption algorithms, focusing on key factors such as Years, Structure, Rounds, Optimal Encoding, Time Evaluation, Memory, Key-Size, Entropy, and Attacks. For visualizations in Python, we utilized the Matplotlib and Seaborn packages. Matplotlib is a 2D plot visualization library for Python that is written in Python and utilizes the NumPy library. Seaborn, on the other hand, is a Python-based dataset-oriented library designed to create various statistical representations built on top of Matplotlib.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Implementation

The project was created using Python and incorporates Jupyter Notebook for visualization. It was constructed on top of the PyCharm platform.

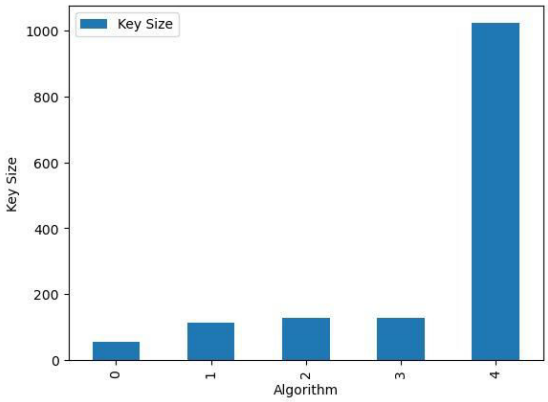
As with any implementation, the initial step involves retrieving the dataset and preparing it for model implementation. This process typically involves the following three steps:

Step 1: Importing the necessary library files

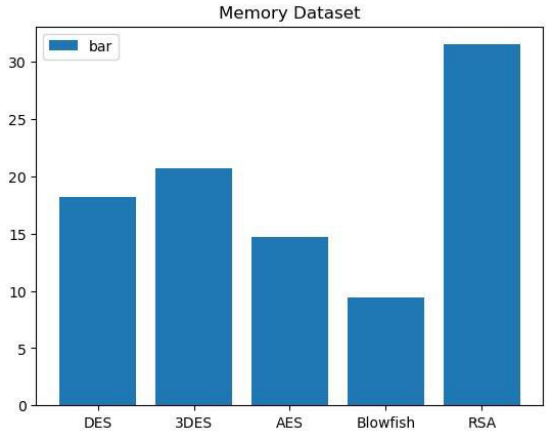
Step 2: Inputting the data via CSV files

Step 3: Generating plots based on the data provided in table format.

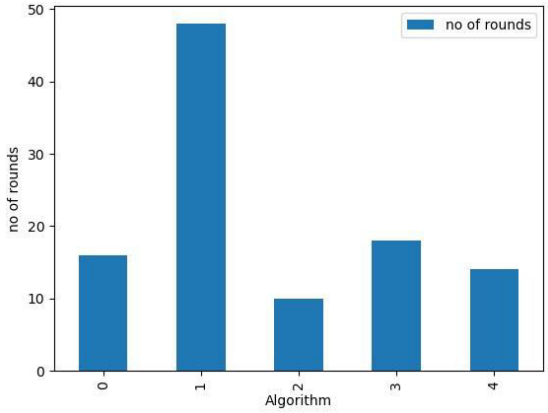
Results



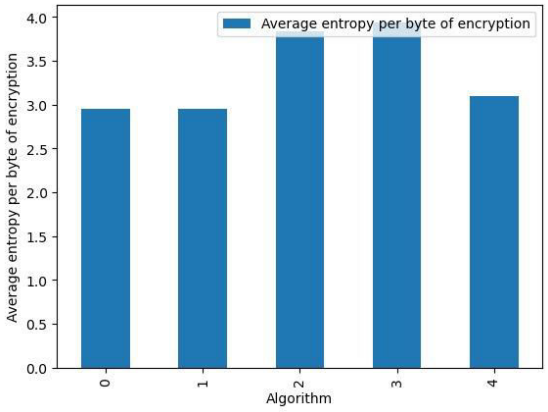
The chart is based on different encryption algorithms, including DES(0), Triple DES(1), AES(2), Blowfish(3), and RSA(4), and their corresponding key sizes. The findings reveal that RSA has the largest key size among all the presented algorithms.



The chart is based on different encryption algorithms and their corresponding memory usage. The findings indicate that the RSA algorithm utilizes more memory compared to the other algorithms presented.



The chart displays different encryption algorithms along with their respective number of rounds. The results demonstrate that the Triple DES algorithm employs a greater number of rounds compared to the other algorithms presented.



The graph is constructed on diverse encryption algorithms and their average entropy bytes per encryption. The outcomes reveal that both the AES and BLOWFISH algorithms possess a higher average entropy when compared to the other algorithms depicted.

Conclusions

By utilizing various encryption techniques such as AES, DES, RSA, and image encryption algorithms, we successfully secured our files. Our comparative analysis revealed a notable pattern in terms of encryption and decryption time, identifying a superior algorithm.To further our study, we included additional algorithms to compare against each other. Additionally, we explored the potential for enhancing security by combining two or more existing algorithms to create a stronger one.

Limitations

This undertaking could serve as a valuable resource for evaluating various encryption methods, identifying their strengths and weaknesses. However, it does have some limitations, which include:

Limited Sample Size: The insufficient number of comparative images may have hindered the ability to draw statistically significant conclusions about the performance of the algorithms.

Lack of Standard Evaluation Metrics: Since there is no universally accepted evaluation metric for comparing encryption algorithms, it may be difficult to draw accurate conclusions from the data analysis.

Limited Encryption Techniques: The comparison could be restricted to only a few particular encryption techniques, which may not be a true reflection of all the encryption algorithms that exist.

Future Scope:

- In the future, research could employ machine learning techniques to assess and compare the efficacy of different encryption algorithms, given the growing popularity of machine learning. One possible approach could be training deep learning algorithms to automatically recognize and classify encrypted images.
- Future research may aim to establish uniform evaluation measures to facilitate a systematic and objective comparison of the effectiveness of various algorithms.

References

[1] Priyadarshini P, Prashant N, Narayan DG, Meena SM. A

Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 2016;78:617-624.

[2] Jeeva AL, Palanisamy V, Kanagaram K. Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering Research and Applications. 2012;2(3): 3033-3037.

[3] Yogesh K, Rajiv M, Harsh S. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. International Journal of Computer Science and Management Studies. 2011;11(3):60-63.

[4] Mahindrakar MS. Evaluation of Blowfish Algorithm based on Avalanche Effect. International Journal of Innovations in Engineering and Technology. 2014;4(1):99-103.

[5] Stallings W. Cryptography and network Security: Principles and Practice. 5th Edition Pearson Education/Prentice Hall; 2011.

[6] Xin Z, Xiaofei T. Research and Implementation of RSA Algorithm for Encryption and Decryption. 6th International Forum on Strategic Technology. 2011:1118-1121.