# Cryptographic Protection With Noise Image As Unique Cipher Key

Anusha.M , Purvika.K , Tanu ,Sai Sambhavi.A

Computer Science Engineering, Dr.Lankapalli Bullayya College of Engineering, Visakhapatnam

## Abstract

To evaluate the performance and security of the proposed system, we conduct experiments using various types of files and noise images. We measure the system's encryption speed, decryption speed, and the level of security achieved. We compare the results with existing file encryption techniques to assess the effectiveness of our proposed system. Additionally, we analyze the system's resistance to common attacks, such as brute force attacks and statistical attacks, to determine its robustness.The research paper concludes by summarizing the findings and discussing the potential applications and future research directions of the proposed system. We highlight the advantages of using noise images as keys in file encryption and decryption, including increased security, ease of key management, and potential applications in multimedia and image encryption. We also identify areas for further research, such as exploring different types of noise images, evaluating the system's performance on large-scale datasets, and investigating the system's resistance to advanced attacks.

**Keywords:** File encryption, decryption, noise image, key generation, information security, image-based encryption.

## 1 Introduction

Information security is a critical concern in to-day's digital world, where sensitive data is constantly transmitted and stored electronically. File encryption and decryption are widely used techniques to protect data from unauthorized access, ensuring confidentiality and integrity. Traditional encryption methods typically use mathematical algorithms and cryptographic keys to trans-form plaintext files into ciphertext and vice versa. However, these methods may have limitations in terms of security, key management, and resistance to attacks.

In this research paper, we propose a file en-cryption and decryption system that utilizes noise images as keys. Noise images are random and chaotic images generated using various techni-ques, such as random number generation, frac-tals, or digital signal processing. By leveraging the unique properties of noise images, we aim to enhance the security and robustness of the file en-cryption and decryption process. The noise image serves as the key that is required to encrypt and decrypt files, adding an additional layer of complexity and randomness to the encryption process.

The proposed system follows an image-based approach, where the noise image is used as the key to transform the original file into a cipher-text, and the same noise image is used as the key to reverse the process and retrieve the original file from the ciphertext. The system consists of three main components: noise image key gene-ration, file encryption, and file decryption. The noise image key generation involves the generation of a noise image using random number gene-ration and image processing techniques. The file encryption process utilizes the noise image as the key to transform the original file into a cipher-text. The file decryption process uses the same noise image as the key to reverse the process and retrieve the original file from the ciphertext.

## 2 Literature Review

Several studies have been conducted on file encryption and decryption techniques. Traditional methods, such as symmetric encryption algorithms (e.g., AES) and asymmetric encryption algorithms (e.g., RSA), have been widely used for securing data. However, these methods have some limitations, such as the need for large key sizes, vulnerability to brute force attacks, and potential vulnerabilities to quantum computing at-tacks in the case of asymmetric encryption. In recent years, researchers have explored alternative methods for file encryption and decryption, such as using biometric information, chaotic sys-tems, and image-based keys. One such approach is using noise image as a key, which has shown promising results in terms of security and robustness.

## 3 Methodology

Our proposed file encryption-decryption sys-tem using noise image as a key consists of the following steps:

### 3.1 Generation of Noise Image Key:

We generate a random noise image using a se-cure pseudorandom number generator, which ser-ves as the encryption and decryption key. The noise image is a matrix of random values that are used to modify the original data.

### 3.2 Encryption Process:

The original file is converted into binary for-mat, and the noise image key is applied as a bitwise XOR operation to modify the binary data. The resulting ciphertext is the encrypted file that can only be decrypted with the correct noise image key.

### 3.3 Decryption Process:

The encrypted file is XORed with the same noise image key to recover the original binary data. The binary data is then converted back into its original format to obtain the plaintext file.

### 3.4 Security Measures:

To enhance the security of our system, we apply additional security measures, such as using multiple iterations of noise image key application, using a strong pseudo-Random number generator, and applying crypto-graphic hash functions for key validation.

### 3.5 Mathematical Principles/Algorithms:

The proposed system is based on the principles of symmetric key cryptography, where the same key is used for both encryption and decryption. The XOR operation is a basic mathematical operation used to modify the original data, and the pseudorandom number generator and cryptographic hash functions are used to generate and validate the noise image key.

## 4 Experimental Results

To evaluate the performance and security of our proposed system, we conducted several expe-riments using different file types and sizes, and compared the results with traditional encryption methods, such as AES and RSA. The experiments included measuring the encryption and decryp-tion time, assessing the security of the system against various attacks (e.g., brute force, chosen plaintext), and evaluating the robustness of the system against noise image key modification or removal. The results showed that our proposed system using noise image as a key provides com-parable or better security compared to traditional encryption methods, with reasonable encryption and decryption times.

## 5 Discussion

Based on the experimental results, we discuss the strengths and weaknesses of our proposed sys-tem. The use of noise image as a key provides an additional layer of security, as the noise image is random and unique

## REFERENCES

1. https://ieeexplore.ieee.org/document/9502246
2. https://ieeexplore.ieee.org/document/9706273
3. https://ieeexplore.ieee.org/document/9315245
4. https://ieeexplore.ieee.org/document/9701774
5. https://ieeexplore.ieee.org/document/9847932
6. https://ieeexplore.ieee.org/document/9681070
7. https://ieeexplore.ieee.org/document/9253112
8. https://ieeexplore.ieee.org/document/9924954
9. https://ieeexplore.ieee.org/document/9835957
10. https://ieeexplore.ieee.org/document/9337031

[1] T. M. K. Afandi, D. H. Fandiantoro, Endroyono and I. K. E. Purnama, "Medical Images Compression and Encryption using DCT, Arithmetic Encoding and Chaos-Based Encryption,"2021 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2021

[2] C. Qin, J. Hu, F. Li, Z. Qian and X. Zhang, "JPEG Image Encryption with Adaptive DC Co-efficient Prediction and RS Pair Permutation,"in IEEE Transactions on Multimedia,2022

[3] M. D and S. Vasuhi, "Image Steganography: 2-Bit XOR Algorithm Used In YCbCr Color Model With Crypto-algorithm,"2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), 2020

[4] J. Tong, Y. Long and Q. Liu, "A File Encryption Sys-tem Based on Attribute Based Encryption,"2021 17th International Conference on Computatio-nal Intelligence and Security (CIS), 2021

[5] A. N, A. V. K and N. R, "Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm,"2022 2nd Internati-onal Conference on Intelligent Technologies (CO-NIT), 2022

[6] H. Nazir, I. S. Bajwa, S. Abdul-lah, R. Kazmi and M. Samiullah, "A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes,"in IEEE Access, 2022

[7] O. Q. J. Al-Thahab and A. A. Hussein, "Implementation Of Stego Watermarking Technique by Encryption Image Based On Turbo Code For Copy-right Application,"2020 1st. Information Techno-logy To Enhance e-learning and Other Applica-tion (IT-ELA), 2020

[8] P. Oktivasari, M. Agus-tin, R. E. M. Akbar, A. Kurniawan, A. R. Zain and F. A. Murad, "Analysis of ECG Image File Encryption using ECDH and AES-GCM Algo-rithm,"2022 7th International Workshop on Big Data and Information Security (IWBIS), 2022

[9] S. Patel and T. V, "New Image Encryption Algorithm based on Pixel Confusion-Diffusion using Hash Functions and Chaotic Map,"2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022

[10] M. E. Kahla, M. Beggas, A. Laouid, M. Kara and M. AlShaikh, "Asymmetric Image Encryption Based on Twin Message Fusion,"2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP), 2021