Journal of Information Systems Engineering and Management
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Image Encryption and Decryption Using XOR operator

G. Rajasekher Reddy[1], P. Lakshmi Vradhan Reddy[2], S. Vishnu Priya[3], P. Anusha Reddy[4], K. Srinivas[5]

[1]*Assistant Professor, Department of CSE, RGMCET, Nandyal, Andhra Pradesh, India, 518501.*
[2] *Department of CSE, RGMCET, Nandyal, Andhra Pradesh, India, 518501.*
[3] *Department of CSE, RGMCET, Nandyal, Andhra Pradesh, India, 518501*
[4] *Department of CSE, RGMCET, Nandyal, Andhra Pradesh, India, 518501*
[5] *Department of CSE, RGMCET, Nandyal, Andhra Pradesh, India, 518501*

ARTICLE INFO

Received: 27 Nov 2024
Revised: 05 Jan 2025
Accepted: 30 Jan 2025

ABSTRACT

Images can be encrypted and contain critical information, just like text. You can employ encryption algorithms such as logistic chaotic maps, RSA (Rivest-Shamir-Adleman), DES (Data Encryption Standard), AES (Advanced Encryption Standard), or even basic scan and XOR-based algorithms. Here is a brief explanation of how XORbased image encryption works and how to scan. The original image is divided into a particular number of blocks. shuffled using scan patterns to generate a new image. Each block's pixels are moved once more. The freshly created image is encrypted using XOR algorithms. Two random blocks from the rearranged image are XORed with each block. A single 128-bit secure key is produced. The designated receiver receives this key, and decryption is carried out. The photos must be encrypted such that they cannot be decrypted without a secure key, even if they are accessed arbitrarily online. You would learn the fundamentals of cybersecurity and hone your cryptography abilities with this assignment.

Keywords: Encryption, Decryption, Cryptography, Cybersecurity.

INTRODUCTION

Computer-based image processing methods help manipulate digital images. In the form of imaging data Satellite platform detectors contain scarcities. Experiencing colourful phases of processing prompts us to look beyond similar excrescences and encourages originality. Pre-processing, improvement and display, and information birth when employing digital fashion, all sorts of data must go through these three general steps. A new fashion is needed for preventing information leakage as a result of the advancement of the data age. For digital data fashion had been developed that is cracking it. This is converting data of readable form into non readable form, in order that if a hacker hack the information he cannot understand it until he know the decryption fashion and decryption word. Now a daysThe digital revolution has altered the average person's way of life. We are on the path to full digitization. Above all, we have saved time and effort by utilizing the digital system for transactions. To communicate from one end to the other, we use a variety of data formats, including voice, audio, and images. There may be a lot of crucial information in this records, particularly for theministries such as defense. As a result, many academics are quite concerned about secure data transport. Visual encryption is one way to hide the original message from unauthorized people. RSA, DSA, block-based scrambling, random grid, Arnold Cat map, R prime shuffle, multilevel encoding, subimage encryption, and many other techniques are presented for visual encryption. Our post discusses one method to achieve this. We have developed a novel algorithm that jumbles the image to provide security when sending the information to a human. We conducted several tests on the scrambled image to evaluate its resilience to different attackers.

A. The use of Encryption

Large amounts of sensitive data are stored and managed on networked computers or in the cloud. Encryption is a cybersecurity tool that guards against ransomware and other assaults, including brute-force attacks. Data encryption protects digital information sent over computer networks and the cloud. Digital data can be divided into two categories: stored digital data and transmitted data, also known as in-flight data, commonly known as data at rest. The antiquated Data Encryption Standard has been superseded by contemporary encryption techniques as the means of data protection. While protecting data, these algorithms provide security features like integrity, authentication, and non-repudiation. The algorithms first authenticate a transmission in order to verify its provenance. After that,

they check for integrity to ensure that the contents haven't changed. Finally, but just as importantly, lawful conduct cannot be rejected by senders due to the nonrepudiation initiative. Many encryption methods have been created with different security needs in mind. The two main types of data encryption are symmetric and asymmetric. Concerns regarding the security of public clouds and safeguarding data in intricate situations are intensifying as more businesses transition to hybrid and multicloud systems. Data on-site and in the cloud can be protected using enterprise-wide encryption and encryption key management. Although cloud service providers (CSPs) may be in charge of cloud security, users are ultimately in control of data security in particular. Sensitive organizational data must be safeguarded while permitting authorized personnel to carry out their duties. In addition to data encryption, this protection should incorporate audit recording, strong access control, and encryption key management. Robust data encryption and key management systems must to provide:

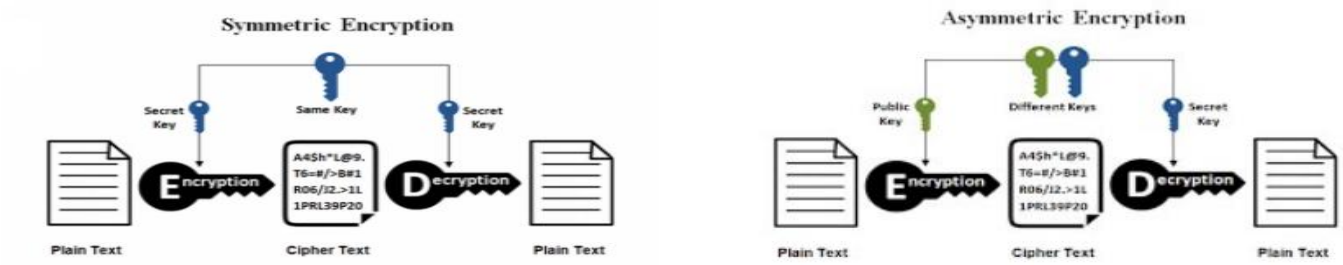
- A centralized console for managing encryption key settings and data encryption.
- Encryption for on-premises and cloud data at the file, database, and application layers.
- Audit logging and role-and group-based access controls are two ways to help with compliance.
- Automated procedures for the key lifetime of cloud and onpremise encryption keys.

B. Decryption

The process of decrypting computer programs is the process of returning data or text that has been encrypted or encoded to its original, easily readable the unadorned version. The reverse of encryption is decryption, which involves encoding data such that only individuals with the appropriate decryption keys can read it. Although the material is protected by encryption, the original details cannot be accessed by receivers without the required decryption or decoding equipment. Decryption is the process of transforming unreadable or indecipherable data into original text files, emails, pictures, user information, and directories that are readable and understandable by computer systems and users. This can be done manually, automatically, with the best decryption software, or with unique keys, passwords, or codes. Decryption is used for a variety of reasons, but one benefit is that it offers sufficient protection. Specifically, this method provides the organization with efficient management. Cyber security experts benefit from the technique since it stops encryption from being used to conflate private data with exfill repetition. Data decryption is the process of returning encrypted data to its original format. In essence, it is a technique for reverse encryption. Because decryption necessitates a secret key or password, it decrypts encrypted data so that only the authorized user can access the message.

C. Cryptography

Building and evaluating methods to counteract adversaries' influence, together with other vibrant information security features like data confidentiality, authentication, and non-repudiation, is a broad description. Electrical engineering, computer science, and mathematics are all impacted by current encryption. Computer passwords, ATM cards, and electronic commerce all use cryptography. In the pre-ultramodern era, encryption—the transformation of data from a legible state to apparent gibberish—was practically synonymous with cryptography. The creator of a translated communication participated in the decoding fashion required to recover the initial information only with intended donors, preventing unauthorized individuals from trying to the same harmonious with this, they will choose a cipher, which means a secret key with the backing of that cipher, they will cipher the Communication. Each letter of the ABC is moved a certain number of times during a Caesar cipher; for example, during a Caesar cipher with a shift of three, A would come D, B would come E, and Y would likewise come B. The Vigenere cipher is made up of a series of` Caesar ciphers with varying shift values. Charles Wheatstone created the Playfair Cipher scheme in 1854. However, Lord Playfair eventually became the name of the plan. The Playfair Cipher, also known as Playfair Square, is a cryptographic method that's employed for inhouse knowledge encryption. These conclusions can be continuously modified because to theoretical advancements like faster computing power and better integer factoring techniques, which is why these schemes are referred to being computationally secure.



D. Need of Security

On mobile devices, data encryption eliminates the risks of loss or theft. Unauthorized users cannot utilise the data as a result of the process. Typically, encryption software transforms data into ”cipher text” by processing it through a mathematical calculation referred to as an algorithm. After this conversion, users must enter their own credentials in order to access the data. They make it nearly impossible for anybody else to access the data if those credentials are kept confidential. Most early computer programs were either completely unsecure or just very loosely secured. This continued for some time before the importance of the data was eventually recognized. In the past, computer data was seen to be beneficial but not something that required protection. When computer programs were developed to handle financial and personal data, the need for security became evident in a way that had never been done before. People understood the importance of computer data in today's world. Consequently, a number of security-related issues began to gain prominence. Two typical examples of these security measures are as follows: Assign a user ID and password to every user, then use those credentials to confirm their identity. Encrypt the data kept in the databases in some way to prevent users without the proper access from seeing it. Technology advancements led to a highly developed communication infrastructure and the emergence of ever-more novel apps to meet the expectations and needs of different user groups. People quickly came to the conclusion that the fundamental security measures were insufficient. In addition, the Internet grabbed the world by storm, and there were several instances of what might occur if applications made for the internet lacked adequate security. Therefore, techniques to safeguard information moving over the internet have been created. Therefore, we are putting out a new technique called the enhanced encryption algorithm, which will make use of two carriers. Carrier1, also known as the Playfair cipher, and carrier 2, also known as the Vigenere cipher, are produced with the use of carrier1 and key` stream generators. Dual security is provided through the use of two carriers, improving the encryption's quality. The primary phases of this method are two. Carrier1 and Carrier2 cipher generation and use with pictures.

LITERATURE REVIEW

Image encryption and decryption play a vital role in securing sensitive image data, particularly in an era where information is frequently transmitted over unsecured networks. Among various encryption methods, the XOR operation stands out due to its simplicity, efficiency, and ability to produce strong results when combined with appropriate keys. This review explores the application of XOR operations in image encryption and decryption, highlighting existing research, methodologies, and advancements. Kumar et al. (2018) carried out an in-depth study evaluating the performance of the Advanced Encryption Standard (AES) algorithm in the context of image security. Their findings underscored AES's strong security capabilities and efficiency, particularly when handling extensive image datasets. This research highlights AES as a highly effective encryption method for protecting digital images.

Sharma and Gupta (2019) introduced an innovative hybrid encryption method that integrates RSA and AES to enhance image security. Their approach demonstrated improved resistance to brute-force attacks compared to conventional encryption techniques. However, they also noted a trade-off, as the hybrid strategy resulted in higher computational costs.

Wang et al. (2020) investigated the use of chaotic maps to develop lightweight encryption methods tailored for real-time image streaming. Their study confirmed that chaos-based encryption enhances randomness in encrypted data. Nevertheless, they emphasized the necessity of precise parameter adjustments to maintain optimal security and encryption efficiency.

Patel et al. (2021) examined the effectiveness of XOR encryption combined with pseudorandom key generation for securing grayscale images. Their research demonstrated that this lightweight encryption method is well-suited for low-power devices. However, they identified a key vulnerability—susceptibility to statistical attacks—which necessitates further improvements to strengthen its security.

Chen et al. (2021) explored the role of quantum key distribution (QKD) in advancing image encryption security. Their study concluded that quantum-based techniques significantly bolster encryption security. However, they also pointed out the major challenge of scalability, which limits the widespread adoption of QKD in practical encryption systems.
Ahmed and Ali (2022) conducted a comprehensive review of image encryption techniques driven by deep learning. Their analysis revealed that AI-based encryption offers dynamic adaptability in encryption parameterization. However, they also highlighted a significant limitation: these methods require extensive computational resources, which may restrict their feasibility in environments with limited processing power.
Raj et al. (2022) proposed a unique pixel-based scrambling technique designed to improve image confidentiality. Their approach proved highly resistant to plaintext attacks while maintaining minimal computational overhead. This efficiency makes the technique suitable for various practical applications requiring secure image encryption.
Taylor and Zhang (2023) investigated the integration of blockchain technology in image encryption and storage. Their findings emphasized the advantages of decentralized storage, which eliminates single-point failures and enhances data security. Additionally, blockchain-enabled traceable encryption ensures an auditable record of encrypted data. Despite these benefits, they acknowledged the added complexity in implementation due to scalability issues, transaction costs, and energy consumption.

A. Introduction to XOR-based Image Encryption

The XOR operation, a fundamental binary operation, is widely used in cryptographic applications. It works by flipping the bits of an input based on the corresponding bits of a key. This operation is particularly advantageous in image encryption due to its reversible nature, lightweight computation, and ease of implementation.

B. Core Principles

The XOR-based encryption process involves the pixel values of an image and a cryptographic key. By performing the XOR operation between these values, the original image is transformed into an encrypted form. Decryption is achieved by applying the same XOR operation using the same key, restoring the original image. The effectiveness of this approach relies heavily on the randomness and secrecy of the key used.

C. Applications and Advantages

- Lightweight Cryptography: XOR operations are computationally efficient, making them suitable for resource-constrained environments such as IoT devices and mobile platforms.
- Real-Time Processing: XOR-based encryption is fast and can handle large datasets, making it suitable for real-time image transmission and processing.
- Noise-Like Cipher Images: The encrypted images generated using XOR operations exhibit randomness, effectively disguising the original content.

D. Research Contributions

Several researchers have proposed enhancements to XOR-based encryption to address potential weaknesses and improve security:

- Key Expansion Techniques: Researchers have emphasized the importance of robust key generation. Techniques like chaotic systems and pseudorandom number generators are integrated with XOR to enhance key unpredictability.
- Cryptosystems: XOR has been integrated with other cryptographic techniques to bolster encryption.

E. Challenges and Limitations

- Key Management: The security of XOR-based encryption heavily depends on the secrecy and distribution of the key. Poor key management can lead to vulnerabilities.
- Known-Plaintext Attacks: XOR encryption can be susceptible to attacks if portions of plaintext are known, as the operation is inherently simple.
- Limited Security with Static Keys: Repeated use of the same key can compromise security, necessitating the development of dynamic key generation methods.

F. Future Directions

- Chaotic Systems Integration: Leveraging chaotic maps to dynamically alter keys during encryption enhances unpredictability and security.

- Quantum Cryptography: Integrating XOR with quantum key distribution (QKD) could pave the way for unbreakable encryption models.
- Adaptive Algorithms: Developing algorithms that adapt to the image content and user-specific requirements can optimize security and performance.

METHODOLOGY

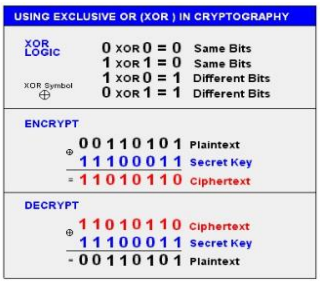
Lorem Although there are numerous ways out there, but here we tried to build the simplest and most secured way in order to perform Encryption and Decryption. The proposed methodology to perform this process is using XOR operation. In here XOR operation is considered to be as one of the Symmetrical Encryption method. We merely create a secret code out of our data or information to guard against unwanted access and to preserve its privacy and security. First, let's examine how the XOR procedure works: An example of an additive cipher, or encryption method that operates contrary to the following rules, is the simple XOR cipher in cryptography:

PROPERTIES OF THE XOR OPERATION

The XOR (exclusive OR) operation satisfies the following mathematical properties:

- Identity Property: XOR-ing any element A with 0 leaves it unchanged:
  $\boldsymbol{A \oplus 0 = A}$
- Self-Cancellation Property: XOR-ing any element A with itself results in 0:
  $\boldsymbol{A \oplus A = 0}$
- Associativity: The XOR operation is associative, meaning the order in which XOR is applied does not matter:
  $\boldsymbol{(A \oplus B) \oplus C = A \oplus (B \oplus C)}$
- Cancellation Property: XOR-ing A with another value B, and then XOR-ing the result again with A, restores B:
  $\boldsymbol{(B \oplus A) \oplus A = B \oplus 0 = B}$

Module 2 addition (or subtraction, which is the same) is another term for this process. According to this reasoning, a text string can be encrypted by bitwise XORing each letter with a specified key. By just utilizing the key to perform the XOR procedure again, you may decode the result and eliminate the encryption. Using the repeating key 11110011, the string "Wiki" can be encrypted and decrypted as follows:

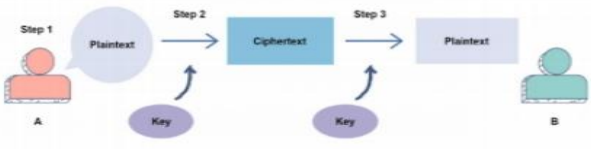


Before delving into the operation of XOR encryption and decryption, it is crucial to establish the foundations of cryptography.

Communication between two endpoints is protected by encryption. For instance, in order to encrypt and decode a message that A wants to transmit to B, both A and B need a key. These are the steps involved:

- The original text message that A intends to convey to B is known as the plaintext.
- The text that A has encrypted using the key is called the ciphertext.
- B will read the message after using the key to change the ciphertext back to the plaintext.

The steps above are shown in the figure below:



Now let's implement the above concept into .The software shown below illustrates the fundamental encryption using XOR operator:

XOR ENCRYPTION AND DECRYPTION IN PYTHON

The following Python code demonstrates how to use the XOR operation for encryption and decryption of data using a key. The same XOR operation is applied for both encryption and decryption due to its symmetric nature.

original_data = 1281 xor_key = 27 # Define the input data and key

print("Original Data:", original_data) print("XOR Key:", xor_key) # Display the original values

Encrypt the data using XOR

encrypted_data = original_data ^ xor_key print("Encrypted Data:", encrypted_data)

Decrypt the data back to its original form

decrypted_data = encrypted_data ^ xor_key print("Decrypted Data:", decrypted_data)

As we can see, the aforementioned program employs two variables: data and a key. The encrypted data is obtained when we first execute an XOR operation on the variables. Then, when we repeat the XOR operation between our data and key (decrypted data), we get the same outcome as our input variable data. The same logic will be applied when encrypting and decrypting a byte array of images. During the encryption process, we will first select an image, then turn it into a byte array. This will turn all of the image data into numeric form, allowing us to perform the XOR operation on it with ease. Now, each time we apply the XOR function to a value, the data will change in the byte array, preventing us from having access to it. However, we must always remember that our encryption key is essential as without it, we are unable to decrypt our image. It functions as a password for decryption. After the encryption process is complete, we will get an encrypted output of our image. Here, the key—which the sender can manually specify throughout the encryption process—will only be known by the sender and the recipient. We can increase our level of security in this way. Furthermore, decryption merely entails converting our encrypted data into a form that can be read. Here, we will decode an encrypted image using the same XOR process. But don't forget that our decryption and encryption keys need to be the same.

RESULTS

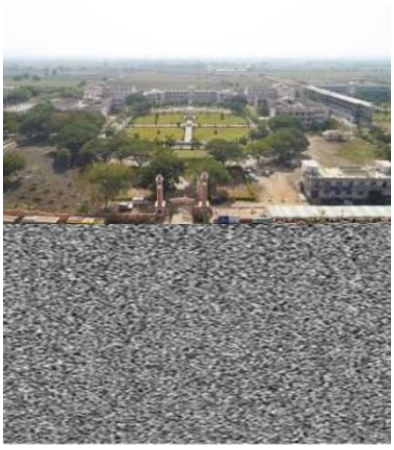


Figure 1 Original and Encrypted File

Figure 2 Decrypted File

Normalized entropy: 0.9603909685706833

When the comparison comes to the Mean, Variance and Entropy values of both Input and Output image files, we obtain results as mentioned below:

Property	Value for Input Image	Value for Output Image
Histogram Mean	118.0634	118.0634
Histogram Variance	4464.0790	4464.0790
Histogram Entropy	5.3255	5.3255

CONCLUSION

In this paper, an image encryption method utilizing the XOR operator is proposed. The results show that the XOR cipher is a useful tool for encrypting images. The original picture's pixel unpredictability increases when we employ the XOR cipher. We can argue that the image is highly secure if the level of randomness is higher. Using a key, the XOR operator is used to odd rows and columns of a picture in order to conflate the relationship between the original and encrypted images. Even rows and columns in the image are assigned the same reversed key. The suggested algorithm's resistance to numerous kinds of attacks, including statistical and differential attacks, has been empirically confirmed by extensive numerical analysis (visual testing). Furthermore, performance evaluation experiments show that the suggested picture encryption approach has a good level of security. It works well for applications involving real-time Internet encryption and transmission due to its rapid encryption and decryption capabilities. Histogram analysis, horizontal and vertical correlation, and information entropy are used to determine that when distinct images are scrambled, the ciphered images become more random, indicating that the ciphered images are more secure and cannot be decrypted. The original photos are encrypted and decrypted using identical security keys. The original image and security key are subjected to an XOR operation in order to encrypt the image. The encrypted image and security key are then subjected to an XOR operation in order to decrypt the image once more. Thus, the use of a security key for decryption depends entirely on the outcome following encryption. Thus, we may say that this procedure makes a picture more secure.

REFRENCES

[1] P. Sharma, D. Mishra, V.K. Sarthi, P. Bhatpahri and R. Shrivastava, "Visual Encryption Using Bit Shift Technique", International Journal of Scientific Research in Computer Science and Engineering, Vol. 5, No. 3, pp. 57-61, June 2017.

[2] XY Wang, YQ Zhang and LT Liu, "An enhanced sub-image encryption method", Optics and Laser in Engineering, Vol. 86, pp. 248-254, November 2016

[3] CC Lee, HH Chen, HT Liu, GW Chen and CS Tsai, "A new visual cryptography with multi-level encoding", Journal of Visual Languages and Computing, Vol. 2,No. 3, pp. 243-250, June 2016.

[4] HB Kekre, T Sarode and P. Halarnkar, "Image Scrambling using RPrime Shuffle", International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, Vol. 2, No. 8, pp. 4070 – 4076, August 2013.

[5] Z. Hua and Y. Zhou, "Design of image cipher using blockbased scrambling and image filtering", Information Sciences, Vol. 396, pp. 97-113, August 2017.

[6] T Guo, F Liu and C. Wu, "k out of k extended visual cryptography scheme by random grids", Signal Processing, Vol. 94, pp. 90-101, January 2014.

[7] X.Y. Wang, F. Chen and T. Wang, "A new compound mode of confusion and diffusion for block encryption of image based on chaos", Communications in Nonlinear Science and Numerical Simulation, Vol. 15,No. 9, pp. 2479-2485, September 2010.

[8] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", Communications in Nonlinear Science and Numerical Simulation, Vol. 17, No. 7, pp. 29432959, July 2012.

[9] C.Y. Song, Y.L. Qiao and X.Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos", Optik, Vol. 124, No.18, pp. 3329-3334, September 2012.

[10] N. Singh and A. Sinha, "Optical image encryption using improper Hartley transforms and chaos", Optik, Vol. 121, No. 10, pp. 918- 925, June 2010.

[11] A. Akhshani, S. Behnia, A. Akhavan, H.A. Hassan and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps", Optics Communications, Vol. 283, No. 17, 3259- 3266, September 2010.

[12] X. Y. Wang, Y.Q Zhang, and L.T. Liu, "An enhanced sub-image encryption method", Optics and Laser in Engineering, Vol. 86, pp. 248-254, November 2016.

[13] B. Stoyanov, and K. Kordov, "Image Encryption Using Chebyshev Map and Rotation Equation", Entropy, Vol. 17, pp. 21172139, April 2015.

[14] X. Tong, Y. Liu, M. Zhang, H. Xu and Z. Wang, "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps", Entropy, Vol. 17, pp. 181-196, January 2015.