Intelligent System to Secure the Information based on Innovative Games

Pooja B[1], Dr. Jalesh Kumar[2], Bhavana R M[3], Dhathri Krishna V[4], Nisarga S[5]

Department of CSE, JNN College of Engineering

1. poojab3112@gmail.com 2. jaleshkumar@jnnce.ac.in 3. rmbhavana2003@gmail.com 4. dhathrikrishnav@gmail.com 5. nisargas541@gmail.com

Corresponding author: poojab3112@gmail.com

Abstract

Cryptography, while essential for data security, faces challenges such as interception during transmission, potentially exposing information to unauthorized parties. To combat this, game-based cryptography techniques have emerged, offering innovative solutions to safeguard sensitive data. This project focuses on developing security models inspired by popular games like Sudoku puzzles. These models aim to enhance data security while engaging users through interactive gameplay. As encryption gains increasing significance amidst rising data breaches and cyber threats, traditional methods often lack user engagement and accessibility. The proposed game-based encryption approach seeks to address these shortcomings by providing a more intuitive and interactive means of securing data across various complexity levels. By integrating puzzle elements into the encryption process, the project aims to bridge the gap between encryption experts and general users, making data security more understandable and engaging for everyone.

Keywords : Cryptography, Encryption, Information, Games

Introduction

Securing information in today's digital landscape presents formidable challenges, requiring safeguarding the data and also maintaining integrity and authentication. With technology advancements, protecting data from illegitimate access becomes increasingly complex, especially as much information is conveyed through images. Image encryption emerges as a pivotal solution, concealing data within images to achieve authentication and deter unpermitted access. This technique adds an extra layer of security, making it hard for intruders to discern hidden data within images. Recognizing the growing importance of encryption amid escalating cyber threats, this project proposes a game-based encryption approach to address existing challenges and offer a more user-friendly solution. By integrating game elements like puzzles into the encryption process, the project aims to democratize data security, by making it accessible and understandable for users across varying expertise levels. The envisioned outcome is a game-based encryption system that not merely ensures robust security but also delivers a seamless user experience. By merging encryption principles with engaging game mechanics, this initiative strives to enhance data and information security.

Literature Survey

A literature survey is crucial in research, offering a comprehensive review of existing knowledge. It identifies gaps, trends, and methodologies, shaping research questions and design. By demonstrating awareness of prior work, it boosts research credibility and aids in result interpretation. It fosters critical thinking, enabling synthesis of information and deeper understanding. In essence, a literature survey informs, guides, and validates research, enhancing its quality and relevance.

The paper [1] introduces various image encryption algorithms, including novel chaotic, permutation-substitution, and grayscale methods. These algorithms aim to enhance Fridrich's structure-based encryption by reducing redundancy. Rubik's Cube principles underpin the design of digital images, emphasizing confusion and diffusion for heightened security. Encryption evaluation involves tests like NPCR and UACI. Additionally, the paper delves into cryptographic algorithms like AES, DES, and RSA, emphasizing their significance in modern cryptography. Dating back to ancient times, cryptography has evolved into a core element of data security, with widespread global utilization. Despite persistent hacking threats, encryption techniques offer robust defense mechanisms, ensuring the data integrity and privacy, even amid potential breaches.

In [2], This work introduces innovative chaotic-based encryption algorithms for multimedia data transmission, surpassing traditional methods. It proposes perturbation-based encryption utilizing 2D alteration models, ensuring high security. The hybrid chaotification structure combines multiple chaotic maps for encryption, offering key sensitivity and low residual clarity. Extensive security and differential analyses confirm the schemes' efficiency and resistance to attacks. Statistical evaluations demonstrate their ability to maintain low residual intelligibility with excellent recovered statistics. Comparative performance against state-of-the-art algorithms highlights the superiority of the recommended schemes, especially in data-specific scenarios. Overall, these novel chaotic-based encryption schemes present a significant advancement in multimedia cryptography, offering enhanced security and performance compared to traditional methods.

In [3], This paper introduces an innovative and lossless image encryption algorithm employing a Sudoku Matrix for scrambling and encrypting images effectively. The algorithm operates in three stages: generating a reference Sudoku matrix, modifying pixel intensities using this matrix, and shuffling pixel positions based on the Sudoku matrix. In contrast to previous methods this algorithm utilizes a complete Sudoku solution for encryption, broadening the matrix concept to any N by N size. Additionally, it incorporates a 1D Chaotic Logistic Map for generating random-like Sudoku matrices. The encryption process dramatically alters the histogram of the encrypted image, ensuring enhanced security. Decryption follows a reverse process, utilizing a security key to regenerate the Sudoku reference matrix. The algorithm's sensitivity to secret keys and large key space makes it resilient against statistical and brute force attacks. Moreover, its encryption and decryption algorithms are easily implementable in hardware.

In [4], The paper introduces a unique image encryption method using a Sudoku puzzle as the encryption key, blending symmetric and asymmetric cryptography techniques. This adaptable algorithm can handle various data types, Sudoku sizes, and keyspaces. It employs modified thresholding with a pseudo-random number from the Sudoku as the threshold, padding the image to match the Sudoku's dimensions, and shuffling rows and columns. Each iteration includes rotating the image by 90 degrees, resulting in strong encryption resistant to brute-force attacks, with a processing time of around 25 milliseconds per iteration for a 512x512 colored square image. The encryption approach contributes a symmetric-key block cipher encryption technique based on Sudoku patterns. It works on data blocks matching the Sudoku size, utilizing multiple rounds of encryption with a transposition cipher for added security. The algorithm is flexible, accommodating custom key spaces, different Sudoku sizes, and user-provided keys. Encryption steps involve reading the image, selecting the Sudoku size, determining encryption rounds, thresholding, padding, shuffling, and iterating through encryption rounds. Decryption reverses the encryption steps, and the algorithm's security relies on a large key size and complex key combinations, making it resilient to brute-force attacks.

In [5], Many chaos-based image and video encryption proposals aim to reduce computational effort and address security concerns regarding conventional ciphers' correlation between adjacent pixels. However, our experimental findings challenge these motivations. Conventional encryption consistently outperforms chaos-based schemes in terms

Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

of computational efficiency. The argument for chaos-based encryption's superior security over traditional ciphers is flawed, as state-of-the-art ciphers prove highly secure when implemented correctly. We focus on image encryption techniques, crucial for video encryption. We classify encryption methods using two-dimensional chaotic maps directly or combining them with generated pseudo-random bit streams. Experimentally, metrics used to assess encryption security fail to distinguish between secure and deliberately insecure schemes.

Design Methodology

Algorithm for Image Encryption based on Sudoku:

1. Generate an Initial Sudoku Matrix at the sender's side.
2. Solve the Sudoku matrix to obtain a solution matrix, which serves as the encryption key.
3. Read the image to be encrypted.
4. Resize the encryption key to match the dimensions of the image.
5. Encrypt the image using the key by performing bitwise XOR operations to produce the cipher text. For colored images, encrypt each color channel separately.
6. At the receiver's side, decrypt the cipher using the same key and algorithm to retrieve the original image.

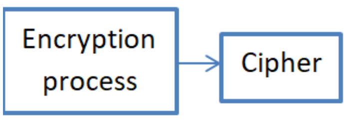

Fig 1: Encryption Process

Fig 2: Decryption Process

Model usage:

Step 1: At sender side.

1. Read the image to be encrypted.
2. Utilize the trained model to implement innovative game algorithm.
3. Using the algorithm encrypt the image.
4. Communicate the key along with the encrypted image through secure channel as cipher.

Step 2: At receiver side.

1. Obtain the key together with the encrypted image through secure channel.
2. Utilize the algorithm
3. Decrypt the cipher image using the key and algorithm to procure the original image.

Results and Analysis

Here, various game-based encryption techniques are devised and implemented within this section. The results obtained in the technique are presented in this chapter. Fig 4 shows the results obtained from Sudoku method.

Fig 3(a) 3(b) 3(c)

Fig 4: Encryption process using Sudoku

PSNR Analysis:

Input Images	Value
3a	28.3413
3b	28.4710
3c	29.1610

The evaluation conducted for three distinct images based on the peak signal to noise ratio (PSNR) resulted in insightful findings. The PSNR values are calculated between input images and their respective encrypted counterparts. The values are tabulated for the method. Low value in the PSNR signifies that it is not possible to identify the original input image on the basis of encrypted image and encrypted image is completely different. There won't be any indication in the encrypted image to infer the original input image.

Correlation Coefficient :

Input Images	Value
3a	0.01008
3b	0.00631
3c	0.00959

The evaluation conducted for three distinct images based on correlation coefficient resulted in insightful findings. The correlation values are computed between input images and corresponding encrypted images. The values are recorded for the method. Low value in the coefficient of correlation indicates that it is not possible to identify the original input image on the basis of encrypted image and encrypted image is completely different. There will be no discernible hints in the encrypted image to deduce the original input image.

Entropy :

Input Images	Value
3a	7.5802
3b	7.5716
3c	7.5841

The evaluation conducted for three distinct images based on entropy resulted in insightful findings. The entropy values are computed between input images and corresponding encrypted images. The values are tabulated for three different methods. High value in the entropy indicates that it is impossible to identify the original input image on the basis of encrypted image and encrypted image is completely different. There will be no discernible hints in the encrypted image to deduce the original input image.

Conclusion

Nowadays, with rapid technological advancements, safeguarding our data from unpermitted access poses a significant challenge. Various technologies have emerged to guarantee the security of sensitive information. This study primarily focuses on utilizing different games to enhance data security. Methods employed in solving games like Sudoku are adapted to safeguard data from unauthorized access. Leveraging techniques derived from these games proves effective in ensuring the confidentiality of sensitive information through game-based cryptography.

References

[1] Dilip Kumar Sharma, Amala Nirmal Doss, "A review on various cryptographic techniques & algorithms", ELSEVIER, 2021

[2] Yasser, Ibrahim and Mohamed, Mohamed A and Samra, Ahmed S and Khalifa, Fahmi, "A chaotic-based encryption/decryption framework for secure multimedia communications", vol 22, 2020, MDPI .

[3] YueWua, YicongZhoua , Joseph P. Noonana , Karen Panettaa , SosAgaian, "Image Encryption using the Sudoku Matrix", Proc. of SPIE Vol. 7708 77080P-1,2017.

[4] Kanaad Deshpande, "Security enhancement and analysis of images using a novel Sudoku-based encryption algorithm", Journal of Information & Telecommunication, 2023.

[5] Mario Preishuber, "Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption", IEEE, 2018.