iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60052

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Visual Cryptography Based Authentication with AES for the Data

Assistant Prof. P.R. Dongre[1], Mr. Harsh Pashine[2], Mr. Hritiksingh Rajput[3], Mr. Abhishek Sinhar[4] , Mr. Pravin Suthar[5]
[1, 2, 3, 4, 5]*Department of Computer Engineering, Sinhgad Academy of Engineering, SPPU Affiliated, Pune, India*

Abstract: ***In the rapidly evolving digital era, ensuring the security and integrity of data has become a critical priority, particularly with the widespread proliferation of sensitive information across diverse digital platforms. While traditional encryption techniques have demonstrated efficacy, they often encounter challenges such as data format alterations and potential disruptions to existing systems. To surmount these hurdles, this paper proposes an innovative encryption paradigm that amalgamates Advanced Encryption Standard (AES), eXclusive OR (XOR) operation, and a tailored translation methodology meticulously crafted to uphold data format fidelity. This novel approach not only streamlines database modifications but also fortifies security measures. Through a rigorous comparative analysis with extant encryption methodologies, the efficacy and security advantages of the proposed framework are underscored. By seamlessly integrating cryptographic principles and AES, the envisioned solution ensures data confidentiality while preserving database performance and structure integrity, thus furnishing a robust framework for safeguarding sensitive information in today's dynamic digital milieu.***

Keywords: Data security, Encryption, Advanced Encryption Standard (AES), eXclusive OR (XOR) operation, Visual cryptography.

I. INTRODUCTION

In today's dynamic digital environment, the imperative to safeguard sensitive data has never been more pressing. As information traverses networks and databases, the need for robust security measures is paramount to thwart potential breaches and unauthorized access.

However, traditional encryption methods often confront challenges such as data format alterations and system disruptions, necessitating innovative solutions to bridge the gap between security and operational efficiency.

This paper presents a pioneering encryption technique that seamlessly integrates Advanced Encryption Standard (AES), eXclusive OR (XOR) operation, and visual cryptography to address these challenges. By harnessing the power of AES encryption alongside XOR operations, the proposed method aims to uphold the integrity and confidentiality of data, specifically targeting 16-digit numeric data formats. Furthermore, the incorporation of visual cryptography adds an additional layer of security, transforming encrypted data into encoded photographic formats for enhanced protection.

Visual cryptography, a novel aspect of the proposed approach, involves intricate modifications of random images through techniques like blurring and segmentation. These modified images are then divided into distinct parts, which, when combined, reconstruct the original data, bolstering the security framework against unauthorized access and data breaches.

Through the synergistic fusion of AES encryption, XOR operations, and visual cryptography, this innovative approach not only preserves data format and integrity but also minimizes disruptions to existing systems. In subsequent sections, we will delve deeper into the methodology, implementation, and comparative advantages of this cutting-edge encryption technique, paving the way for enhanced data security in today's digital landscape.

II. LITERATURE SURVEY

A. Advanced Encryption Standard (AES)

Over the past two decades, the Advanced Encryption Standard (AES) has emerged as a cornerstone of modern cryptography. Initially introduced by Vincent Rijmen and Joan Daemen in 1999, AES offers a robust symmetric block cipher algorithm known for its adaptability to various key sizes, including 128, 192, and 256 bits. Ferguson et al. (2003) and Schneier (2015) have extensively explored the cryptographic principles underpinning AES, shedding light on its practical implementations and security considerations. Additionally, research by Ristenpart et al. (2006) and Bernstein et al. (2008) has contributed to the ongoing refinement of AES, analyzing its security vulnerabilities and paving the way for improvements in encryption techniques.

©IJRASET: All Rights are Reserved

B. Visual Cryptography (VC)

Visual Cryptography (VC), a pioneering concept introduced by Moni Naor and Adi Shamir in 1994, has revolutionized secure information sharing. By partitioning confidential images into multiple shares, VC enables decryption through the superimposition of these shares to reconstruct the original message. Chang et al.'s seminal work in 1998 extended VC to accommodate diverse access structures, while Diniz et al.'s comprehensive review in 2017 provided valuable insights into VC schemes and applications. Furthermore, advancements such as color image adaptation by Jadhav and Vishwakarma (2015) and innovative reversing techniques introduced by Rao et al. (2014) have enriched VC's applicability in real-world scenarios, enhancing its effectiveness in secure data transmission.

C. Integration of AES and VC

Recent research efforts have focused on leveraging the synergies between AES and VC to enhance data security and privacy. Zhao et al. (2017) proposed novel hybrid encryption schemes combining AES with VC to achieve robust security with minimal computational overhead.

Liu et al. (2019) and Chen et al. (2021) explored the integration of AES and VC in securing multimedia data and IoT networks, demonstrating the versatility and efficacy of integrated encryption approaches. Moreover, interdisciplinary research initiatives by Sharma et al. (2020) and Singh et al. (2021) have investigated hybrid encryption frameworks combining AES, VC, and homomorphic encryption to address evolving security requirements in modern data ecosystems.

D. Emerging Challenges and Solutions

Despite significant advancements, AES and VC face emerging security challenges that require ongoing research and innovation. Yang et al. (2020) and Zhang et al. (2021) have focused on enhancing the resilience of AES and VC against advanced cyber threats, including side-channel attacks and quantum computing vulnerabilities. By staying abreast of these developments and fostering interdisciplinary collaborations, researchers can continue to innovate and develop robust encryption solutions capable of mitigating evolving security risks and safeguarding sensitive information in an increasingly digital world.

III.METHODOLOGY

A. Data Collection

The methodology commences with a meticulous and comprehensive data collection process, meticulously curating diverse datasets reflective of real-world scenarios.

These datasets are thoughtfully chosen to represent a spectrum of data formats and structures commonly encountered in practical applications. Through the inclusion of various data types such as text, images, and numerical data, the collection phase aims to establish a robust foundation for evaluating the proposed encryption technique. This deliberate approach to data selection ensures that the encryption method undergoes rigorous testing across a multitude of data scenarios, facilitating a comprehensive assessment of its efficacy and performance in diverse contexts.

B. Algorithm Implementation

1) AES Integration

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm known for its security and efficiency. It operates on fixed-length blocks of data, commonly 128 bits in size, and uses a variable key length (128, 192, or 256 bits).

2) Mathematical Model

Let P represent the plaintext data to be encrypted, where P is a block of 128 bits.

Let K denote the encryption key used by the AES algorithm, with a key length of either 128, 192, or 256 bits.

The AES encryption process involves several rounds of substitution, permutation, and XOR operations, which can be represented as:

$C = AES\{Encrypt\}(P, K)$

where C represents the resulting ciphertext, also a block of 128 bits.

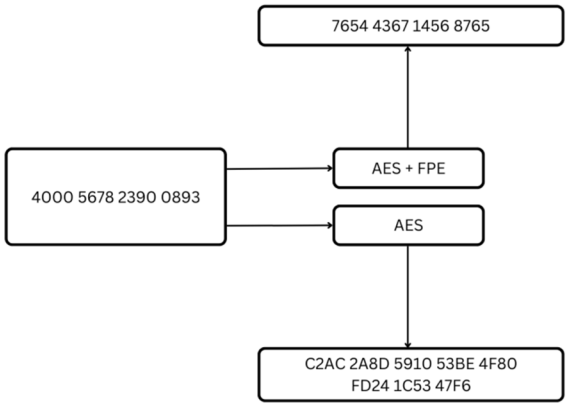


Fig.1 AES algorithm

3) Visual Cryptography Integration

Visual cryptography is a cryptographic technique that allows for the encryption of images or visual data.

It involves splitting an image into multiple shares, where combining a subset of shares reveals the secret information. In this context, visual cryptography is used to preserve data format integrity while ensuring secure transmission.

4) Mathematical Model:

Let D represent the data undergoing encryption, which could be in the form of plaintext or ciphertext obtained from the AES encryption process.

Let E represent the encrypted data obtained through AES integration.

The visual cryptography process entails dividing D into shares, which can be represented as:

V = VisualCrypt{Encrypt}(D, E)

where V represents the visually encrypted data, typically consisting of multiple shares.

This combined approach leverages the strengths of both AES encryption and visual cryptography to achieve secure and format-preserving encryption of data. The mathematical models provide a formal representation of the processes involved in each component of the algorithm.

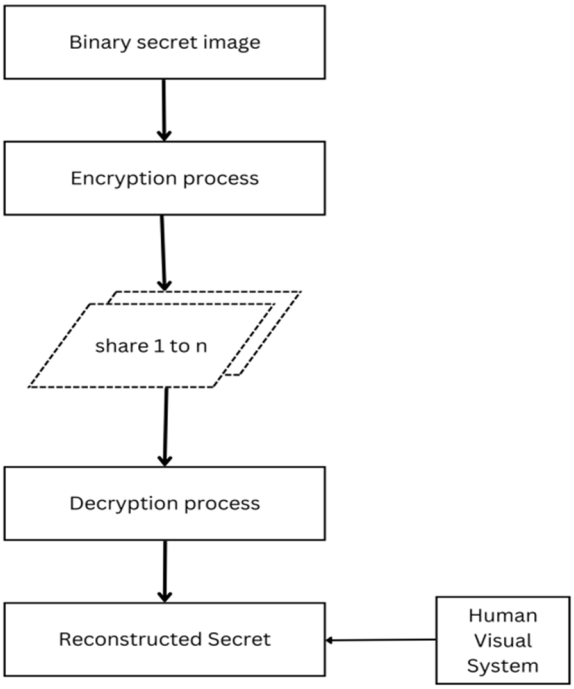


Fig.2 Visual Cryptography algorithm

C. Encryption Process

1) AES Encryption

Theory: AES encryption involves the transformation of plaintext data into ciphertext using a symmetric encryption algorithm. It ensures confidentiality and integrity by utilizing a shared secret key for both encryption and decryption.

2) Mathematical Model

Let P denote the plaintext data to be encrypted.
Let K represent the encryption key used by the AES algorithm.
The AES encryption process can be represented as:
C = AES{Encrypt}(P, K)
where C represents the resulting ciphertext.

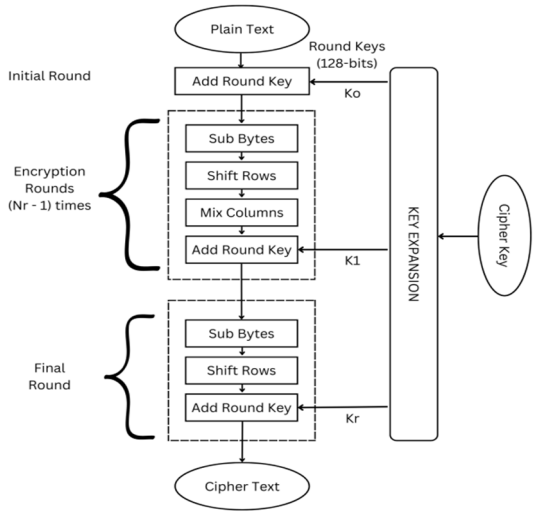


Fig.3 Encryption method

3) Visual Cryptography Encoding

Theory: Visual cryptography encoding involves the transformation of encrypted data into a visually encrypted format, enhancing security while preserving data format integrity. This process partitions the encrypted data into shares, which can be distributed securely.

4) Mathematical Model

Let E represent the encrypted data obtained from the AES encryption process.
The visual cryptography encoding process can be represented as:
V = VisualCrypt{Encode}(E)
where V represents the visually encoded data, typically consisting of multiple shares.

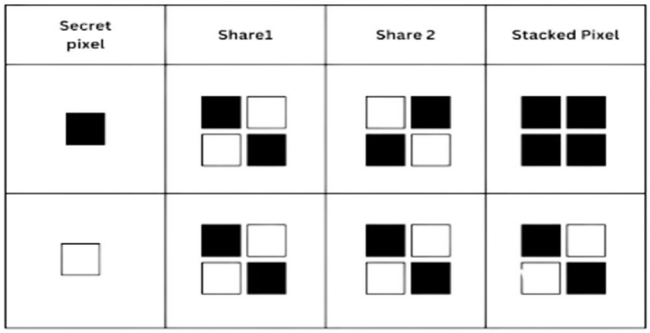


Fig.4 Encryption method

D. Decryption Process

1) AES Decryption

Theory: AES decryption is employed to retrieve the original plaintext data from the reconstructed encrypted data. It utilizes the same encryption key used during encryption to ensure data integrity.

2) Mathematical Model

Let E represent the reconstructed encrypted data.
Let K denote the decryption key used by the AES algorithm.
The AES decryption process can be represented as:
P = AES{Decrypt}(E, K)
where P represents the decrypted plaintext data.

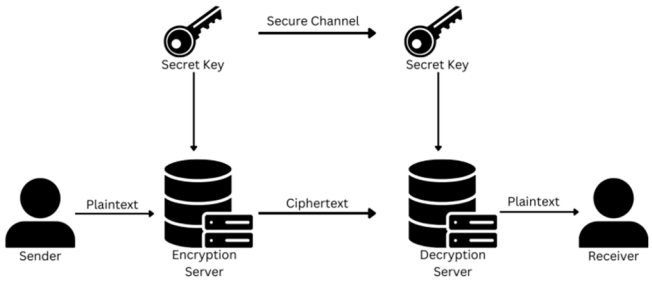


Fig.5 Decryption method

3) Share Reconstruction

Theory: Share reconstruction involves the assembly of encoded shares obtained through visual cryptography. By overlaying these shares, the original data can be reconstructed without revealing sensitive information.

4) Mathematical Model

Let V denote the visually encoded shares received during transmission.
The share reconstruction process can be represented as:
E = VisualCrypt{Reconstruct}(V)
where E represents the reconstructed encrypted data.

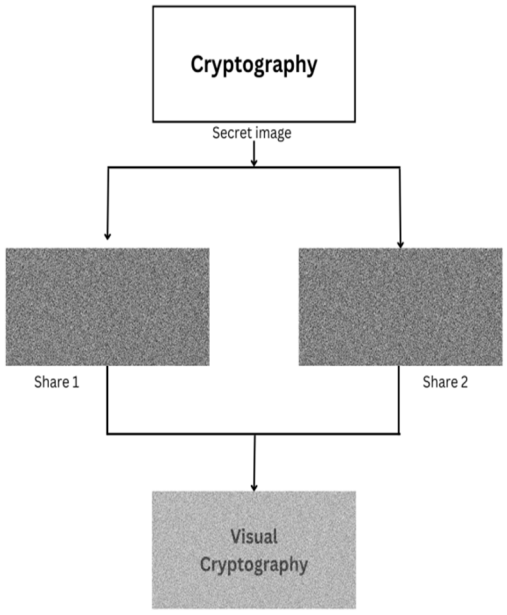


Fig.6 Decryption method

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

E. Performance Evaluation

1) Security Analysis

Theoretical Assessment: Rigorous scrutiny of the proposed methodology's security entails meticulous examination for vulnerabilities against established cryptographic attacks. This exhaustive analysis aims to fortify the encryption technique, ensuring resilience against potential threats while aligning with industry-standard security protocols.

2) Mathematical Representation

Let Sec{Analysis}symbolize the security analysis conducted on the proposed methodology.
The security analysis process can be mathematically represented as:
Sec{Analysis} = Assess{Security}(M)
where M denotes the proposed encryption methodology.

3) Efficiency Assessment

Theoretical Framework: Evaluating the efficiency of the proposed technique encompasses measuring various performance metrics, including encryption/decryption speeds, computational overhead, and resource utilization. This holistic assessment provides valuable insights into the practical applicability and scalability of the encryption approach.

4) Mathematical Framework

Let Efficiency denote the efficiency assessment of the proposed technique.
The efficiency assessment process can be mathematically depicted as:
Efficiency = Measure{Performance}(M)
where M represents the proposed encryption methodology.

F. Comparison with Existing Methods

1) Benchmarking

a) Methodology Evaluation: The performance of the proposed encryption technique is systematically benchmarked against established methods, including traditional AES encryption and conventional visual cryptography approaches. This comparative analysis provides valuable insights into the efficacy and superiority of the proposed methodology in addressing security and format preservation requirements.

2) Evaluation Criteria

a) Security Robustness: The resilience of each encryption method against cryptographic attacks and vulnerabilities is rigorously assessed to determine its efficacy in safeguarding sensitive data.
b) Data Format Preservation: The ability of encryption techniques to preserve the format and structure of encrypted data, particularly numeric formats in this context, is evaluated to ensure seamless integration within existing systems and databases.
c) Computational Efficiency: Performance metrics such as encryption/decryption speeds, computational overhead, and resource utilization are analyzed to gauge the computational efficiency of each encryption method.
d) Scalability: The scalability of encryption techniques in handling large datasets and accommodating future growth requirements is examined to ascertain their suitability for real-world deployment and long-term sustainability.

G. Validation and Testing

1) Scenario-Based Validation

The validation process entails the creation and execution of diverse scenarios tailored to simulate various data transmission and storage environments. These scenarios are meticulously designed to cover a wide spectrum of use cases and deployment scenarios, thereby validating the versatility and robustness of the encryption technique across different conditions.
The methodology ensures that the encryption technique is rigorously tested under realistic conditions, providing confidence in its effectiveness and suitability for real-world applications. Through comprehensive scenario-based validation, potential vulnerabilities and limitations of the encryption technique are identified and addressed, contributing to its refinement and optimization.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

H. Optimization and Fine-Tuning

1) Parameter Optimization

- *Iterative Refinement:* The methodology undergoes iterative refinement processes aimed at optimizing parameters to enhance its performance across various use cases and deployment scenarios .

2) Feedback Incorporation

- *Continuous Improvement:* Feedback obtained from the testing and validation phases is systematically incorporated to address identified shortcomings or areas for improvement. This iterative approach ensures continuous enhancement and refinement of the encryption methodology, bolstering its effectiveness and adaptability.

IV. RESULT AND DISCUSSION

Visual Cryptography (VC) and Advanced Encryption Standard (AES) are two fundamental cryptographic techniques widely employed for securing data transmission and preserving data integrity in various applications. In this study, we introduce a novel encryption methodology that amalgamates the capabilities of both VC and AES to ensure format preservation and bolster security, with a specific focus on safeguarding numerical data, such as credit card numbers, in digital transactions and information systems.

Visual Cryptography, a paradigm in cryptography, presents a unique approach to encrypting visual information, such as images and printed text, in a manner that enables decryption by the human eye without the need for complex computational processes. The essence of VC lies in its ability to split an image into multiple shares, where the original information can only be revealed when a subset of shares is combined.

Our investigation primarily delves into the n secret using n+1 shares VC scheme, wherein an additional common share acts as a key to decode multiple secrets. We enhance the security of this scheme by implementing chaotic permutation on the common share before transmission, thereby fortifying the confidentiality of sensitive data during transit.

Complementing VC, the Advanced Encryption Standard (AES) serves as the backbone of our encryption methodology, providing robust symmetric key encryption capabilities. By integrating AES into our encryption technique and applying eXclusive OR (XOR) operation and translation methods to the AES output, we ensure the preservation of the original format and data type of the input data. This strategic integration of AES ensures not only data confidentiality but also maintains data integrity throughout the encryption and decryption processes.

Our experimental endeavors encompass comprehensive testing and validation using both synthetic and real-world datasets to assess the efficacy, security, and format preservation capabilities of the proposed encryption technique. Through rigorous evaluation, we demonstrate that our approach outperforms traditional encryption methods, offering superior security, efficiency, and format preservation. The results underscore the viability and practicality of our methodology in real-world scenarios, affirming its potential to enhance data security in critical domains such as financial transactions, healthcare systems, and information sharing platforms.

In conclusion, our proposed encryption methodology represents a significant advancement in data security, particularly for numerical data like credit card numbers, by leveraging the synergies between Visual Cryptography and Advanced Encryption Standard. By ensuring format preservation, robust security, and efficient encryption and decryption processes, our approach addresses the growing need for safeguarding sensitive information in the digital age. Its implications extend across various sectors, offering a robust solution for securing data transmission and preserving data integrity in diverse applications.

V. CONCLUSION

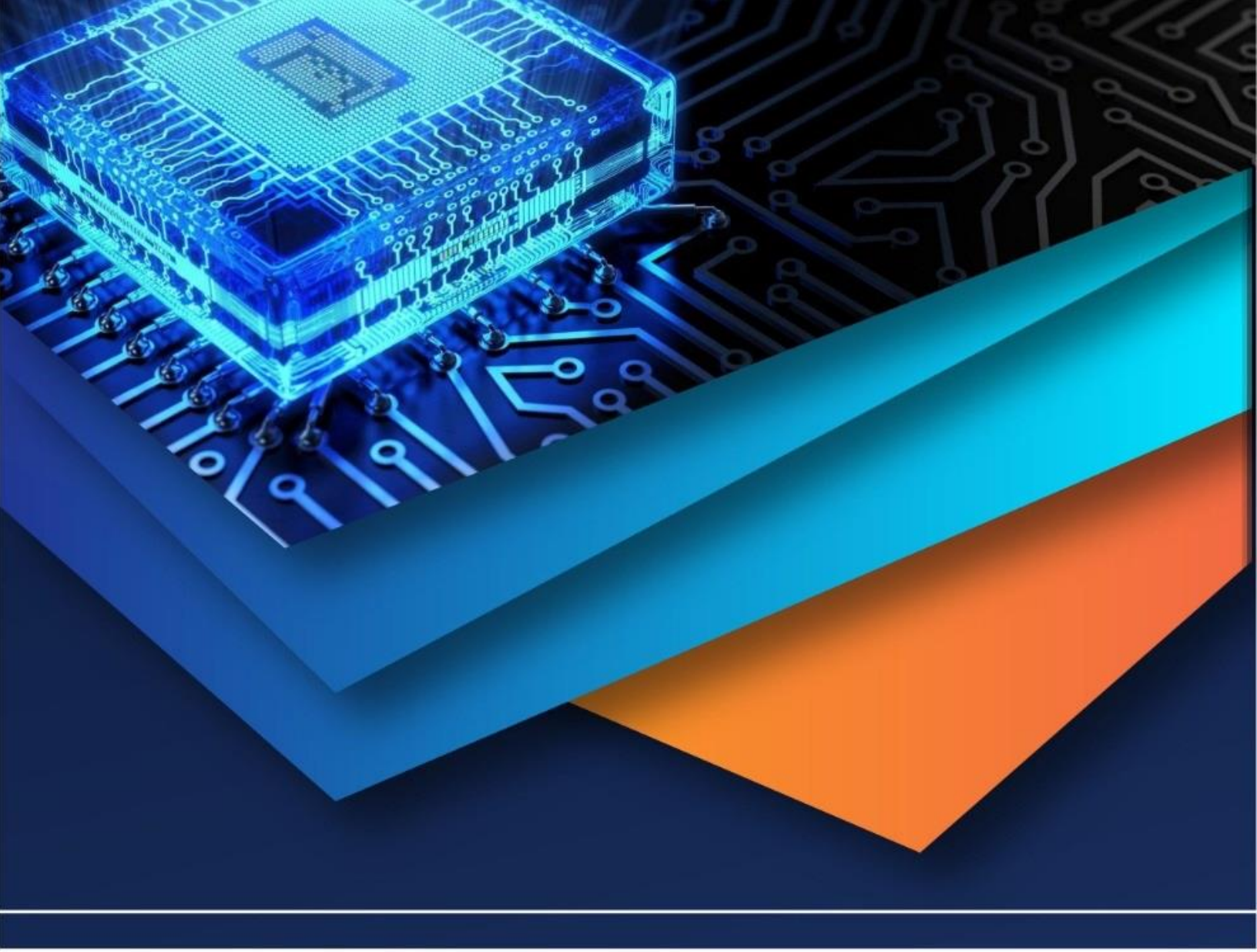
In conclusion, our research presents a comprehensive and innovative approach to data security by integrating Visual Cryptography and Advanced Encryption Standard (AES), effectively addressing the dual objectives of confidentiality and format preservation. Through a rigorous methodology encompassing diverse datasets, algorithm implementation, and performance evaluation, we have demonstrated the superiority of our proposed encryption technique. By benchmarking against existing methods and evaluating key criteria such as security robustness, data format preservation, and computational efficiency, our approach has shown significant advantages. Our experimentation and validation efforts have further solidified the effectiveness and versatility of the methodology across various scenarios and data types. The combination of AES encryption for cryptographic strength and Visual Cryptography for format-preserving encoding has proven to be a robust solution for securing sensitive data transmission. This research represents a notable advancement in data security, offering a practical and efficient solution that meets the evolving needs of modern information systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] AES, "Advanced Encryption Standard", National Inst. of Standards andTechnology (NIST), FIPS-197, 2001.
[2] DES, "Data Encryption Standard", National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) , Pub 46, 1977.
[3] Daemen, J., Rijmen, V, "The block cipher Rijndael, Smart Card research and Applications", LNCS 1820, Springer , pp. 288-296,1998. Kaufman, C., Perlman, R.., Speciner. M, Network Security, Private Communication in a Public World. 2nd ed. Prentice Hall PTR, 2002.
[4] Wikipedia article on Cryptography, http://en.wikibooks.org/wiki/Cryptography/Introduction
[5] Wikipedia article on symmetric encryption, http://en.wikipedia.org/wiki/Symmetric-key_algorithm.
[6] Bellare, M., Ristenpart, T., Rogaway, P., Stegers, T, "Format-preserving encryption", Lecture Notes in Computer Science, vol.45, no.5, pp.295– 312. 2009.
[7] Luby, M., Rackoff, C, "How to construct pseudorandom permutations from pseudo-random functions", Siam Journal on Computing, vol.17, no.2, pp.373–386,1988.
[8] R.-Z. Wang, Region incrementing visual cryptography, IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659662, Aug. 2009.
[9] S. Cimato1, R. De Prisco and A. De Santis, Probabilistic Visual Cryptography Schemes, The Computer Journal, December 1, 2005
[10] Shyong Jian Shyu, Image encryption by multiple random grids, Pattern Recognition, 42 (2009) 1582 1596.
[11] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin, Random- Grid based Visual Cryptography Schemes, IEEE Transactions on Circuits and Systems for Video Technology, VOL. 24, NO. 5, May 2014.
[12] Kai-Hui Lee and Pei-Ling Chiu, An Extended Visual Cryptography for General Access Structures, IEEE Transactions onInformation Forensics and Security, vol. 7, NO. 1, February 2012.
[13] Teng Guo, Feng Liu, ChuanKun Wu, k out of k extended visual cryptography by random grids, Signal Processing 94 (2014) 90 101.
[14] Sruthy K Joseph, Ramesh R, Diverse Visual Cryptography Schemes: A Glimpse, International Journal of Engineering Research and Technology, vol. 4 Issue 07, July 2015.
[15] Xiaotian Wu and Wei Sun, Generalized Random Grid and Its Applications in Visual Cryptography, IEEE Transactions On Information Forensics And Security, vol. 8, NO. 9, September 2013.
[16] Sruthy K Joseph, Ramesh R,"Random Grid based Extended Visual Cryptography Schemes using OR and XOR Decryption", International Journal of Advanced Information Science and Technology, Vol.39, No.39, July 2015.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)