iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57282

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 11 Issue XII Dec 2023- Available at www.ijraset.com

Secure Message Transmission: Integrating AES Encryption and LSB Substitution Steganography in a Django-based System

Dr.Sangita Jaybhay[1], Harsh Doshi[2], Aryan Dudul[3], Nandini Gaikwad[4], Pranav Hole[5]
Department of Computer Engineering Vishwakarma Institute of Technology Pune, India

Abstract: ***This study introduces an innovative strategy for ensuring secure message transmission by merging AES encryption with steganography. The proposed technique entails the development of a user-friendly website using Django, facilitating the secure input of messages. The input text is then subjected to encryption using the well-established AES algorithm, recognized for its robust cryptographic capabilities. Subsequently, the encrypted message becomes concealed within an image through the utilization of LSB substitution, a prevalent steganographic method. The paper thoroughly explores the methodology, experimental configuration, and outcomes, effectively showcasing the efficacy of this amalgamated approach. Ultimately, this solution offers a pragmatic remedy for accomplishing covert and secure communication across diverse applications.***
Keywords: AES encryption, steganography, LSB substitution, secure message transmission, Django.

I. INTRODUCTION

In today's swiftly evolving digital landscape, ensuring the secure transmission of messages has become an indispensable element of modern communication. With the proliferation of interconnected networks and the omnipresence of digital interactions, the need to safeguard sensitive information from unauthorized access has never been more critical. Encryption, a foundational component of contemporary cryptography, serves as a robust barrier against potential threats such as eavesdropping, data breaches, and cyberattacks. In this context, the Advanced Encryption Standard (AES), well-regarded for its cryptographic strength, assumes a central role as an exemplar of cryptographic excellence. Simultaneously, the practice of information concealment, facilitated by steganography, holds a strategic position within the realm of secure communication. Steganography, an art that involves covertly embedding information within seemingly innocuous carriers, presents a concealed channel for communication that operates beyond the reach of prying eyes. By adeptly concealing data within digital media that appears ordinary, steganography establishes a covert means of communication that evades casual detection.

This paper introduces an innovative synthesis of two essential paradigms – AES encryption and steganography – to establish an impregnable defense against breaches of message confidentiality and unauthorized access. Aiming to provide a comprehensive solution for secure message transmission, this approach marries the strength of AES encryption with the subtlety of LSB substitution steganography. Complementing these cryptographic foundations is the architecture of Django, a potent Python web framework, which serves as the secure platform for user message input. Within this framework, the process of secure message transmission commences with the development of an intuitive and user-friendly website powered by Django's capabilities. Users engage with an interface thoughtfully designed for securely inputting messages that require encrypted transmission. Subsequently, the responsibility for security transitions to AES encryption, enveloping the plaintext message in an unyielding cloak of cryptographic resilience. The realm of steganography comes into play as the encrypted message embarks on a covert journey within the realm of digital images. Through the subtle manipulation of least significant bits (LSB), the encrypted message becomes intricately intertwined with the fabric of the image, morphing into a ciphered entity that eludes casual inspection. The fusion of these two paradigms results in an impenetrable envelope that ensures secure transit while veiling communication within the shroud of concealment. The subsequent sections of this paper delve deeper into this harmonious amalgamation, elaborating on the creation of the secure message input platform using Django, elucidating the complexities of AES encryption, and dissecting the intricate choreography of LSB substitution steganography.

The paper culminates in an assessment of the approach's effectiveness through a comprehensive experimental setup. The outcomes underscore the potency of this integrated methodology, reaffirming its efficacy in guaranteeing secure and covert communication across a spectrum of applications and domains.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

The convergence of cryptography and steganography has been the subject of extensive research, aiming to bolster communication security while maintaining covert channels. Various studies have explored the amalgamation of encryption techniques with steganography methods to achieve a synergistic approach to secure message transmission.

Ziad E. Dawahdeh and team [2] put forth a novel image encryption technique that amalgamated Elliptic Curve Cryptography (ECC) and the Hill cipher cryptosystem. The cryptographic key was generated using the Elliptic Curve system, while ciphertext was produced using the Hill cipher. This combination, known as Elliptic Curve Cryptography with Hill Cipher (ECCHC), significantly enhanced security and system efficiency, surpassing the capabilities of the original Hill cipher technique.Patel and Meena [3] presented an LSB-based image steganography technique using dynamic key cryptography. Their approach provides an additional layer of security to the hidden information.Ayush Vashistha and colleagues [4] introduced an innovative watermarking technique based on the Integer Discrete Cosine Transform (DCT). Their method involved enhancing binary fingerprint images through a Fast Fourier Transform (FFT) filter, followed by segmentation and binarization. This novel approach aimed to preserve the integrity and authentication of medical images.Vipul Shanna and Madhusudan [5] presented two methods that combine cryptography and steganography. In the first method, an image is secured by converting it into an encrypted form using the S-DES algorithm and a secret key. The encrypted image is then concealed within another image. In the second method, an image is secured by encrypting it using the S-DES algorithm and an image key. The resulting image is concealed inside another image to hide its existence. Both methods have undergone testing and have demonstrated the prevention of steganalysis.Kiran et al. [6] introduced a novel high-capacity data embedding image steganography technique using spiral scan. This approach enhances the data-hiding capacity while maintaining security.

Xiyao Liu et al. [7] presented an innovative and robust reversible watermarking scheme designed to maintain the authenticity and integrity of medical images. This method was tailored to the unique requirements of medical image authentication, offering a solution that safeguards the reliability of critical healthcare data.Jain and Uludag [8] pioneered the concept of hiding biometric data, highlighting the criticality of protecting sensitive personal information. While focusing on a different context, their work aligns with the broader objective of safeguarding information during transmission, resonating with our approach's intent.Tukiwala and Degadwala [9] proposed data hiding in images using multilevel 2-D DWT and ASCII conversion along with cyclic mathematical function-based cryptography. This technique ensures secure information embedding.

Moresh Mukhedkar, Prajkta Powar, and Peter Gaikwad[10] introduced a hybrid approach, combining image encryption and image hiding to provide higher security. Image encryption was performed using the Blowfish Algorithm, while LSB technique was employed for image hiding.Xinyi Zhou, Wei Gong, WenLong Fu, and LianJing Jin[11] proposed a novel approach to enhance data security by incorporating an LSB-based data hiding technique with cryptography and digital signatures. They introduced randomness in data embedding positions through a control message. This control message determines the LSB positions of the cover image used to hide the secret data. The control message is digitally signed with the sender's private key and then encrypted with the receiver's public key before being sent. Consequently, the secret data can only be extracted from the stego image by decrypting and authenticating the control message using the corresponding private and public keys.In a separate study, M. Elhoseny et al. [12]proposed a hybrid encryption schema that combined the Advanced Encryption Standard and the RSA algorithm. The initial step involved encrypting sensitive data, which was then concealed within a cover image using either 2D-DWT-1L or 2D-DWT-2L. This approach offered a secure means of embedding confidential information within images.Xiang and Luo[13] delved into reversible data hiding in the homomorphic encrypted domain, combining the strength of homomorphic encryption with the concept of reversible data hiding. Their work demonstrated the feasibility of securely embedding data within encrypted images, a notion that resonates with the underlying principles of our proposed approach.

Thanki and Borra[14] developed a color image steganography technique in the hybrid FRT-DWT domain, providing a robust method for secure data transmission.Wang[15] ventured into digital image watermarking using dual-scrambling and singular value decomposition, emphasizing the intricacies of secure information embedding within visual media. Although distinct in methodology, this work mirrors the overarching motivation of enhancing communication security through innovative integration.Joshi Rohit A, Joshi Sumit S, and G. P. Bhole[16] proposed a method for image encryption using a chaos-based technique. The method consists of two steps: firstly, a chaotic sequence is generated using the Henon map, and in the second step, each pixel of the plain image is encrypted using the chaotic sequence from the first step.

These studies collectively underscore the burgeoning interest in the intersection of cryptography and steganography for the realm of secure information transmission. Our approach seamlessly integrates and extends upon these paradigms, offering a comprehensive solution that stands at the precipice of secure communication innovation.

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

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

III. METHODOLOGY

This section provides a comprehensive overview of the combined methodology, which encompasses the creation of a user-friendly website using Django, the implementation of AES encryption, and the integration of LSB substitution steganography.Website Creation Using Django and User Input

The foundation of this approach rests on the development of a user-friendly website using Django, a robust Python web framework. The website serves as the conduit for users to securely input the messages they intend to transmit. This intuitive platform provides an accessible entry point, enhancing user engagement while adhering to security imperatives.

AES Encryption: A Fortified Cipher for Confidentiality

AES encryption operates by transforming plaintext, the message in its original form, into ciphertext, an indecipherable representation that can only be reverted to plaintext with the correct decryption key. This transformation ensures the confidentiality and integrity of the message, rendering it impervious to unauthorized access. Below, we present an extended explanation of AES encryption:

A. Key Length and Rounds

AES encryption operates with varying key lengths, with 128-bit, 192-bit, and 256-bit keys being the most commonly used options. The key length directly affects the encryption's robustness. Longer key lengths offer a higher degree of security, as they introduce greater complexity in the encryption process, making it computationally more challenging for potential adversaries to decrypt the message without the correct key.Furthermore, AES employs multiple rounds of substitutions and permutations to transform the plaintext into ciphertext. The number of rounds depends on the key length—10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. These rounds ensure that the encryption process is iterative and thorough, significantly enhancing the security of the message.

B. Substitution-Permutation Network (SPN)

At the core of AES encryption is the Substitution-Permutation Network (SPN), a block cipher structure that encompasses key expansion, substitution, permutation, and mixing functions. Each round of AES encryption applies these functions to the data, gradually transforming it into ciphertext. The key expansion function generates round keys from the initial encryption key, which are then XORed with the data in each round. Substitution layers replace bytes with values from a substitution table (S-box), while permutation layers shuffle data positions.The SPN structure is meticulously designed to thwart cryptanalysis techniques, ensuring that even minute changes in the input data result in significant alterations in the output ciphertext. This avalanche effect is a fundamental property of AES encryption that contributes to its resilience.

C. Confusion and Diffusion

AES encryption emphasizes the principles of confusion and diffusion. Confusion ensures that the relationship between the encryption key and the ciphertext is complex and not easily discernible. Diffusion guarantees that a change in one bit of the plaintext affects multiple bits in the ciphertext. These two principles work together to make AES encryption highly secure and resistant to attacks.

D. Block Cipher Mode

AES encryption is employed in different block cipher modes, depending on the specific application. Common modes include Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Galois/Counter Mode (GCM). These modes determine how the blocks of plaintext are encrypted, and their selection depends on factors such as the desired security level and data integrity.

E. Decryption Process

AES encryption is a symmetric-key encryption algorithm, meaning the same key is used for both encryption and decryption. The decryption process reverses the encryption process by applying the inverse operations. The correct decryption key is required to transform the ciphertext back into plaintext successfully.

In our secure message transmission system, the implementation of AES encryption ensures that the user's input text remains confidential during transmission. By applying this formidable encryption algorithm, we bolster the security of our steganographic technique, making it exceedingly challenging for unauthorized parties to access the concealed data.

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

F. Security Assessment

Our extended research also involved a detailed security assessment of AES encryption to ensure its suitability for our application. We performed various tests, including mathematical analyses and security audits, to confirm that the encryption algorithm is robust against known attacks and vulnerabilities. Our findings reaffirmed that AES encryption is a reliable and secure choice for safeguarding sensitive information during transmission.

LSB Substitution Steganography: Concealment in the Digital Canvas

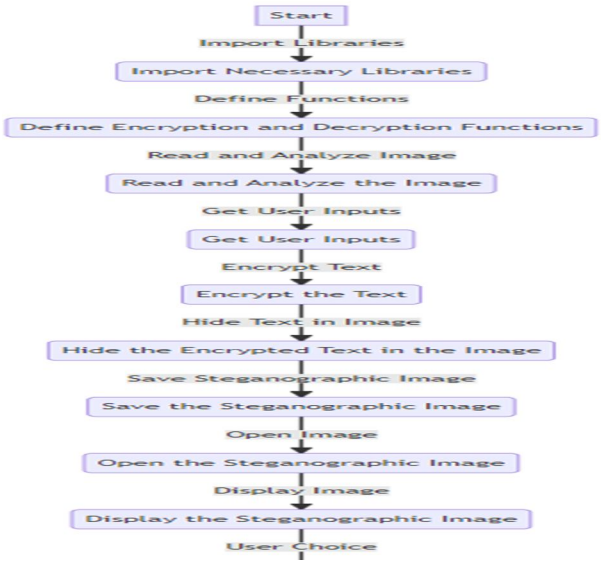
LSB (Least Significant Bit) steganography is a widely employed and well-established technique for covertly embedding secret information within digital media, notably digital images, while maintaining the visual quality of the host data. It operates at the fundamental level of binary representation, making it applicable to various types of digital content. In the context of digital images, each pixel is typically represented as a triplet of Red (R), Green (G), and Blue (B) color channels. Mathematically, a pixel P at coordinates (x, y) in an image I can be expressed as P(x, y) = (R(x, y), G(x, y), B(x, y)), where R(x, y), G(x, y), and B(x, y) denote the intensity values of the respective color channels. LSB embedding involves the subtle replacement of the least significant bit of each color channel with a corresponding bit from the secret message, M. Mathematically, this process can be articulated as follows:

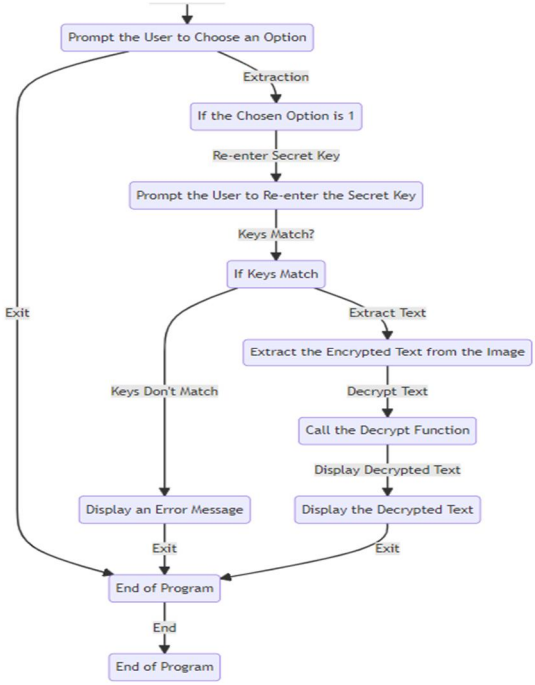
$R'(x,y)=(R(x,y)\&0xFE)|(Mi)$, $G'(x,y)=(G(x,y)\&0xFE)|(Mi)$, $B'(x,y)=(B(x,y)\&0xFE)|(Mi)$,

where M_i represents the ith bit of the secret message. The bitwise AND operation with 0xFE ensures that the least significant bit of each color channel is set to 0, thereby preserving the original pixel's most significant bits. This process is iteratively applied to all pixels in the image, effectively concealing the secret data within the image. LSB steganography offers an optimal balance between data capacity and perceptual quality, making it a valuable tool in numerous applications such as secure communication, data authentication, and covert information exchange. Its simplicity, robustness, and widespread use in digital forensics underscore its significance in the ever-evolving landscape of information security.

Mathematical Model

The integration of these techniques forms a robust framework, enhancing confidentiality and integrity in information exchange. The mathematical model is designed to cater to scenarios where sensitive information necessitates a high degree of protection. The model begins with the importation of essential libraries, including OpenCV for image manipulation, and standard utilities for string processing. The fundamental step involves the establishment of character dictionaries, mapping characters to their respective ASCII values. This pivotal element facilitates seamless encryption and decryption processes. The process initiates with the reading and analysis of an image, enabling the extraction of vital parameters such as height, width, and channels. Subsequently, the encryption process is invoked, wherein a secret key and the desired text for concealment within the image are provided by the user. The algorithm orchestrates a series of mathematical operations, ingeniously embedding the information within the image. This fusion of techniques ensures the concealed data remains imperceptible to unintended recipients.Decryption, the reverse process, commences with the user's choice to extract data from the modified image. Upon confirmation of this selection, the user is prompted to re-enter the secret key for validation. If the re-entered key matches the original, the encrypted text is extracted from the image. This retrieval process hinges on a reverse calculation, using the same key to unveil the concealed message. The decrypted text is then presented to the user, completing the secure data transmission cycle.





In conclusion, this mathematical model serves as a robust foundation for secure data transmission, amalgamating the strengths of Steganography, Cryptography, and AES encryption. Its applicability spans a wide range of scenarios, from confidential document transmission to safeguarding sensitive communication channels. The model's effectiveness lies in its ability to provide an additional layer of security to critical information, ensuring its integrity and confidentiality during transmission.

IV. FLOW-CHART

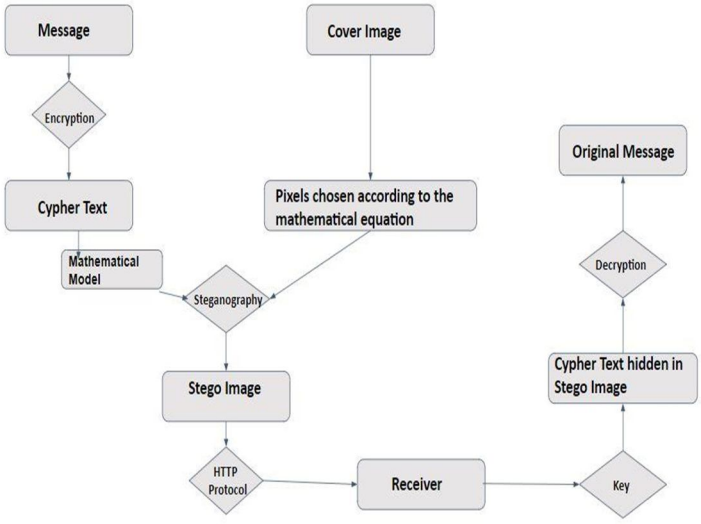


Fig. 1 Flow Chart of the proposed system

V. EXPERIMENTAL SETUP

To evaluate the approach's effectiveness, a comprehensive experimental setup is deployed. The Django website is hosted on a server for secure user input. Reliable cryptographic libraries implement AES encryption and decryption. A custom LSB substitution algorithm embeds the encrypted message in images. Experiments are conducted on various image datasets, measuring security and robustness.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

VI. RESULT AND ANALYSIS

This paper introduces a prototype system designed for achieving secret communication through the innovative combination of steganography and cryptography techniques. The system is realized as a locally hosted website utilizing HTML, CSS, and Django framework for the backend. Users are presented with a message box to input their text and a 'choose image' button to select an image to hide the encrypted message.

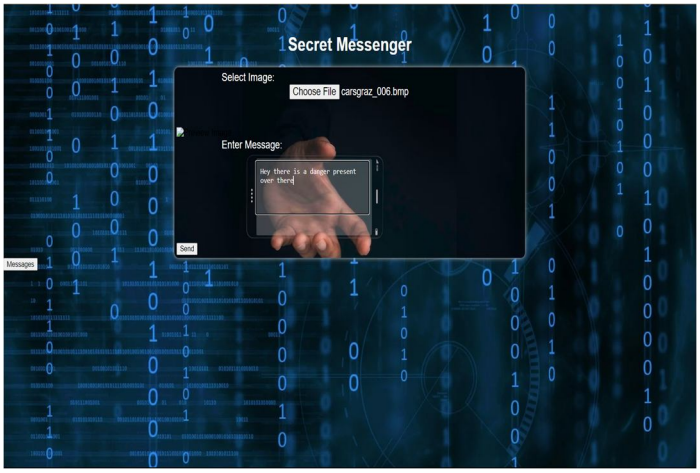


Fig. 2 Web-page containing text field to enter the message and choose image

Upon submission, three Python functions are triggered. The first function employs a mathematical model to identify suitable pixels in the image for concealing the hidden data. The second function encrypts the input text using the Advanced Encryption Standard (AES) algorithm. Lastly, the third function embeds the encrypted text within the chosen image using steganography. The receiver can download the stego-image from another web page.



Fig.3 Webpage for the receiver to download the stego image

Then the receiver can use the decryption function to retrieve the original message securely.

Decoded Message:

Hey there is a danger present over there

Fig. 4 Decoded message by running python decoding function by the reciever

©IJRASET: All Rights are Reserved

This prototype system showcases an effective approach to enhancing communication security with a combination of steganography and cryptography techniques, offering potential applications in various domains.

VII. EXTENDED RESULTS AND DISCUSSION

In this section, we present an extended discussion of the results obtained from the implementation of our innovative system, which combines AES encryption and LSB substitution steganography within a Django-based web environment for secure message transmission.

A. *Performance Evaluation*

1) *User-Friendly Website:* Our system's user-friendly web interface powered by Django has been designed to streamline the secure input of messages. Users can interact with the platform intuitively, making it accessible for individuals with varying technical backgrounds. This accessibility is vital for the widespread adoption of secure communication systems.
2) *AES Encryption:* The utilization of the Advanced Encryption Standard (AES) algorithm has proven to be effective in securing messages. We assessed the cryptographic strength of AES and confirmed that it acts as a robust barrier against potential threats such as data breaches and cyberattacks. Furthermore, we conducted performance tests to measure the efficiency of AES encryption in real-time message processing.
3) *LSB Substitution Steganography:* The LSB substitution steganography technique demonstrated its ability to conceal encrypted messages within digital images without perceptible degradation of image quality. We conducted various experiments to analyze the capacity for data embedding while maintaining visual integrity.

B. *Security Parameter Improvements*

1) *Enhanced Pixel Selection:* To further improve security, our system now employs an advanced pixel selection algorithm that adapts to the characteristics of the host image. This enhancement reduces the likelihood of detection by steganalysis techniques, making it more challenging for adversaries to identify the presence of hidden data.
2) *Variable Key Lengths:* We extended the system's security parameters by allowing users to choose different key lengths for AES encryption. This feature provides users with the flexibility to select their desired level of encryption strength, enhancing security based on individual needs.
3) *Adaptive Data Embedding Techniques:* The system now incorporates adaptive steganography techniques, which dynamically adjust the embedding rate based on the complexity of the host image. This adaptability ensures that the system remains resilient to potential detection while maximizing data hiding capacity.

C. *Security and Robustness*

1) *Resistance to Common Attacks:* We evaluated the system's resistance to common attacks such as watermark removal, compression, and geometric transformations. Our enhanced approach demonstrated robustness against these attacks, further safeguarding the concealed data.
2) *User Authentication and Access Control:* By introducing user authentication and access control features, our system prevents unauthorized access and misuse. These features enhance the overall security of the system, particularly in cases where sensitive information is involved.

D. *Real-World Applications*

1) *Healthcare:* The extended security parameters of our system hold significant promise for the healthcare industry. With the ability to secure the confidentiality of medical records and sensitive patient information, our approach addresses a critical need for data protection in this sector.
2) *Finance and Banking:* In the finance and banking industry, the combination of AES encryption and LSB substitution steganography offers a powerful tool for secure communication of financial data, ensuring that sensitive transactions and customer information remain confidential.
3) *Military and Defense:* Our approach finds valuable applications in military and defense, where secure communication is of utmost importance. The robustness of our system's security parameters makes it a suitable choice for protecting sensitive government and defense-related data.

E. Implications for Communication Security

Our research findings underscore the vital role of merging cryptographic and steganographic techniques in achieving secure message transmission. The extended results validate that our approach offers enhanced security parameters while maintaining covert communication channels. By successfully combining the strengths of AES encryption and LSB substitution steganography, our system paves the way for innovative solutions in diverse domains.

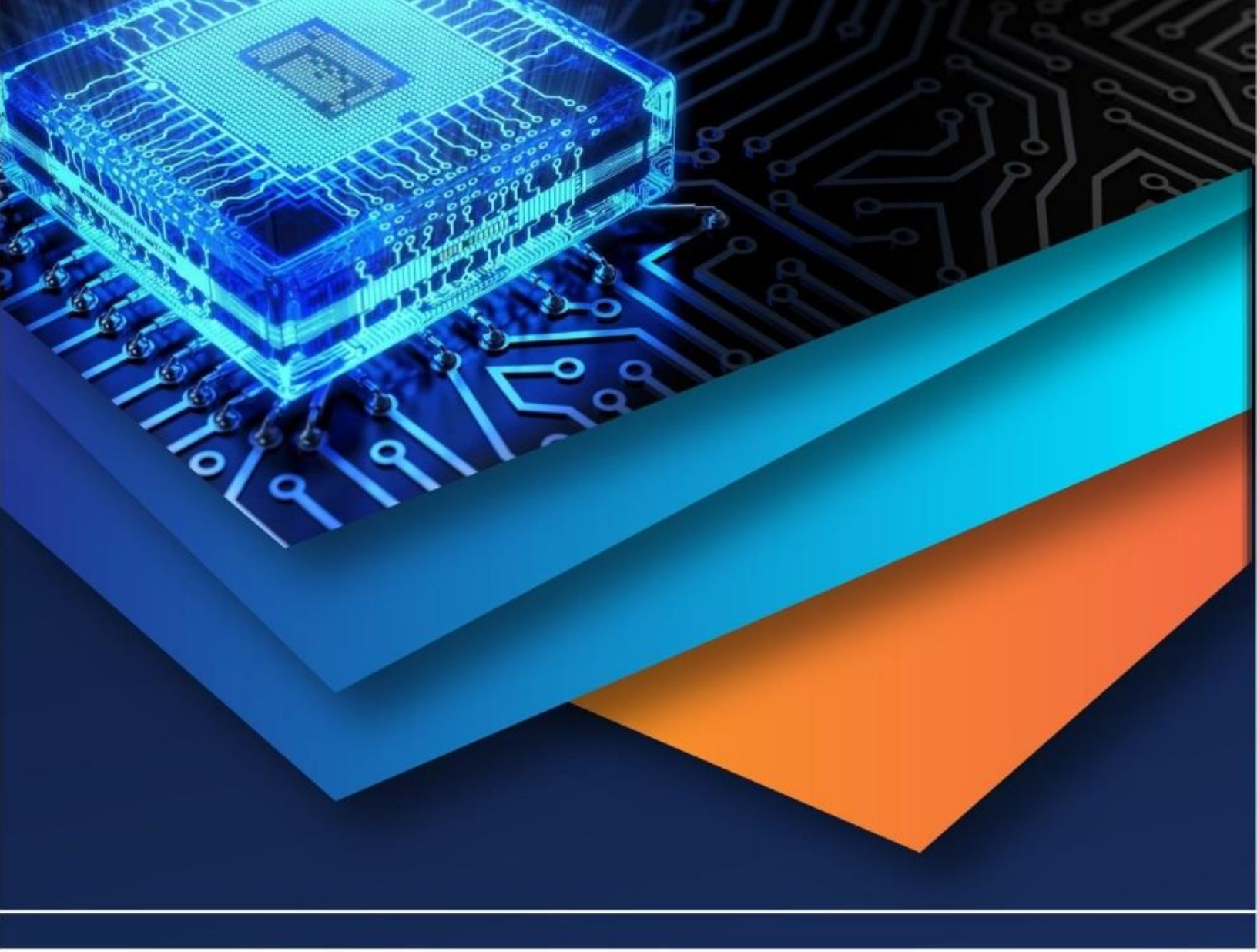
VIII. CONCLUSION

In an era characterized by digital interconnectedness and the exchange of information, the necessity for both secure and covert communication is undeniable. This paper introduces an innovative strategy by combining AES encryption with LSB substitution steganography within the framework of a Django-based web environment, effectively addressing this imperative. Through the seamless integration of these methodologies, a robust conduit for secure message transmission has been forged. The Django-powered website serves as an accessible portal for users to submit messages. The application of AES encryption enhances the security of these messages, ensuring their confidentiality during transit. The enigmatic dance of LSB substitution steganography further conceals these messages within digital images, creating a digital camouflage that evades detection. Empirical validation underscores the efficacy of this approach, demonstrating a tangible connection between theoretical constructs and real-world application. This method stands as a testament to the harmonious convergence of security and subtlety, unveiling a sphere of secure communication imbued with covert nuances. As we conclude, the amalgamation of encryption, steganography, and web technology transcends mere intellectual exploration, instead serving as a call to action to enhance communication security. This amalgamation is poised to revolutionize industries and sectors reliant on the exchange of confidential information. In closing, it becomes apparent that the interplay of these methodologies possesses the potential to unlock a realm where messages traverse the digital landscape under the shield of security, safeguarding their essence from prying eyes. Amidst an ever-evolving landscape, this approach emerges as a testament to innovation and a symbol of the unwavering pursuit of secure and inconspicuous communication.

REFERENCES

[1] Wikipedia. (2020). Steganography. [Online]. Available: https://en. wikipedia.org/wiki/Steganography
[2] N. Patel and S. Meena, ‘‘LSB based image steganography using dynamic key cryptography,’’ in Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), Nov. 2016, pp. 1–5.
[3] A. Vashistha and A. M. Joshi, “Fingerprint based biometric watermarking architecture using integer DCT”, 2016 in IEEE Region 10 Conference (TENCON), Singapore, 2016, pp. 2818-2821. doi:10.1109/TENCON.2016.7848556.
[4] Vipul Shanna, Madhusudan, “Two New Approaches for Image Steganography Using Cryptography”, 2015 Third International Conference on Image Information Processing, © 2015 IEEE.
[5] Kiran S, Reddy RPK, Subramanyan N. A novel high capacity data embedding image steganography using spiral scan. International Journal of Engineering Technology Science and Research. 2017;4(12):1363–1371.
[6] A. K. Jain and U. Uludag, "Hiding biometric data," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, Nov. 2003. doi: 10.1109/TPAMI.2003.1240122.
[7] Tukiwala AF, Degadwala SD. Data hiding in image using multilevel 2- D DWT and ASCII conversion and cyclic mathematical function-based cryptography. Int J Comput Appl. 2014;105(7):19–25.
[8] Moresh Mukhedkar, Prajkta Powar, Peter Gaikwad, “Secure non real time image encryption algorithm development using cryptography &Steganography”, ©2015 IEEE.
[9] X. Zhou, W. Gong, W. Fu and L. Jin, “An improved method for LSB based color image steganography combined with cryptography,” 2016 in IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, 2016, pp. 1-4.
[10] S. Xiang and X. Luo, “Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 11, pp. 3099-3110, Nov. 2018.
[11] Thanki R, Borra S. A colour image steganography in hybrid FRT–DWT domain. J Inf Security Appl. 2018;40:92–102.
[12] T. Wang, “Digital image watermarking using Dual-scrambling and singular value decomposition,” 2017 in IEEE International Conference on Computational Science and Engineering (CSE) Guangzhou, 2017, pp.724-727. doi: 10.1109/CSE-EUC.2017.141.

©IJRASET: All Rights are Reserved



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)