RESEARCH ARTICLE OPEN ACCESS

Image Encryption for Secure Internet Transfer

Mahaveer Parakh*, Dushyantraj Sharma*, Akash Rawat, Jyoti Sain****

*B.Tech Student, Department of CSE, Arya Institute of Engineering & Technology, Jaipur

**Assistant Professor, Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India

ABSTRACT

Most of our data is transferred over the internet nowadays, so data security is important. Cryptography and steganography are two main branches of information security. Cryptography provides encryption techniques for secure communication. There are many cryptographic algorithms, almost all of which are suitable for text encryption. Now it is impossible to communicate only by text, so images, audio and video are used for communication. Steganography involves hiding vital information in images. In addition to steganography, optical cryptography is widely used to prevent the transmission of images or hidden images.However, it is not so safe to achieve color-shared generation. There are also some patterns in the color combination created using many available methods. The encrypted image is then divided into color segments. On the decryption side, all coordinates use the same color scheme and become input to the Visual-AES decryption module to reveal the hidden image.

Keywords: Encryption, Algorithm, Decryption, Key, Visual Cryptography, Password Generator

I. INTRODUCTION

Visual cryptography may be an essential cryptographic strategy that permits visual data such as pictures, content, etc.to be encrypted in a way that decryption becomes the task of someone deciphering it through decryption [1-2]. The concept of encryption is to split an image into n shares so that only a person with all the shares can decrypt the image [3-4], while a share n-1 shows no information about the original image. Each copy is printed separately and a decision is made by placing the copies on top of each other. When all copies are finished, the original image will appear.

The underlying technique has many generalizations, including k-out-of-n visual encryption. Visual cryptography can be used to protect biometric structures where decryption does not require complex calculations [5].Visual cryptography plays an important role in protecting image-based secrets [6-10]. The shared color is created using optical cryptography to encrypt images for shares, and during decryption all shares are combined to reveal the hidden image [11]. Research identified the following differences in the cryptography view:

- Requires multi-level security keys with key symbols to ensure data security.
- The data is subset and must have a superset path so that hackers using level-level security cannot access it.
- The length of the key should not exceed 256 to 512 bytes.
- Changing the RGB entropy needs to be changed to change the pixel position.
- The combination of cryptography and steganography is a good way to ensure security. Increasing the Complexity of Reusing Steganographic Techniques with Image Coding [12-15].

II. PROPOSED SYSTEM

The current color sharing method is to extract the R, G and B components from the Color image and then apply the gray scale color expression generation algorithm to the R component and then combine all the components to get n R gray scale sharing. Joints with B and G components to create the joint color. On the decryption side, components B and G are extracted from each component, then all r gray components are combined into r components, and then all R, G and B are rendered usefully to reveal. hidden photo The decrypted hidden image is the same size as the hidden image. This way, the gray co-creation algorithm is only used for the R component, so the full co-map is not created. It may have a view of the old image, so it's less useful.

There are many different image and text encryption methods. DES is an old method of encrypting data so that it cannot be read by others who can interfere with traffic. DES is old and has been replaced by newer and better AES. The change is due to a weakness in DES that allows accidental access using some attack methods. Currently, the wide use of AES continues for all encryption methods, making it a good choice for high-end encryption.

There is a lot of research to improve the performance of AES. 3D-AES [6] blocks encrypted symmetric cryptographic algorithm for SMS transport security. From the experiment, the encryption time of 3D-AES is very short when the message size is more than 256 bits. This work presents an image security algorithm that combines Visual-AES (a modification of AES) and color segmentation generation.

Encryption process: AES may be a piece cipher expecting to supplant DES for commercial uses and multiple applications. AES calculation is of three sorts i.e. AES-128, AES-192 and AES-256. This classification is done on the bases of the key utilized within the calculation for encryption and decoding handle. The numbers speak to the measure of key in bits. This key measure decides the security level as the estimate of key increments the level of security increments. The AES calculation employments a circular work that's composed of four diverse byte-oriented changes.

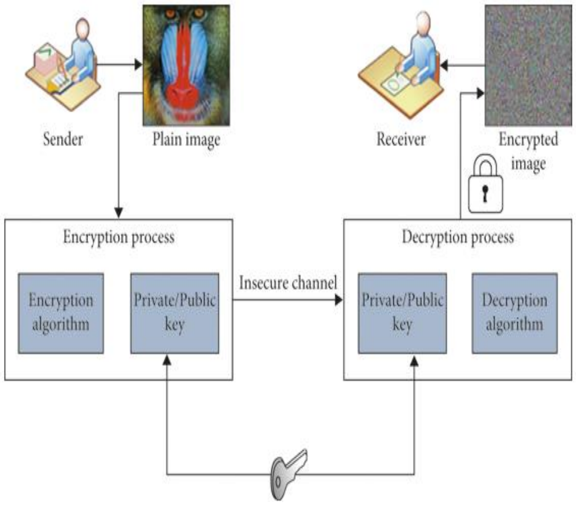

Figure 1. AES Encryption Process

In AES, all operations and commands are performed on 8-bit bytes. In specific, the number juggling operations of expansion, duplication, and division are performed over the limited field GF (2^8). For encryption reason four rounds comprise of:

- • Substitute byte
- • Move row
- • Blend columns
- • Include circular key

The cipher comprises of 10 rounds since this can be a 16-byte key. The primary 9 rounds comprise of four particular change functions: Sub bytes, Move columns, blend columns and Add round key. The ultimate circular contains only three changes, and there's an beginning single change (include circular key) some time recently the primary circular. Each change takes one or more 4*4 lattices as input and produces a 4*4 framework as yield.

Decryption process: AES decryption is the reverse of encryption. Figure 4 shows the flow of the AES decryption algorithm. In the case of decoding the reverse shift byte, the reverse shift line and the reverse shuffle line are used. It stays the same when adding a round key.

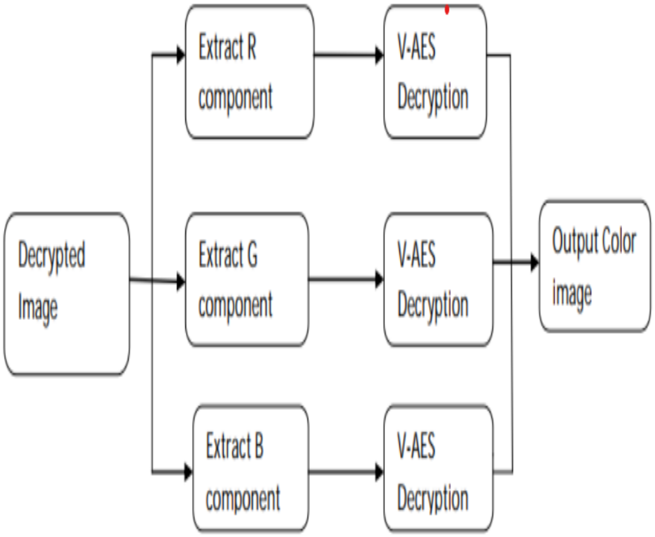

Figure 2. AES Dencryption Process

III. PRACTICAL APPLICATIONS IN FUTURE

A. Discussion on Potential Applications of the Proposed Image Encryption Algorithm:

- Secure Communication: The algorithm can be utilized to secure image transmission in various communication channels, such as email attachments, messaging platforms, or file-sharing services. It ensures that the images remain confidential and protected from unauthorized access during transmission.
- Medical Imaging: Medical institutions can benefit from the algorithm's security features to protect sensitive medical images during their transfer between healthcare providers. This ensures patient privacy and helps prevent unauthorized access to personal health information.
- Military and Defense: The proposed algorithm can find applications in secure image transfer within military and defense organizations. It can protect classified or sensitive imagery during communication between military units or intelligence agencies, preventing adversaries from intercepting or tampering with the images.
- Financial Institutions: The algorithm can be utilized to secure the transfer of financial documents containing images, such as bank statements, transaction receipts, or digital signatures. This helps protect against fraud, data breaches, and unauthorized access to financial information.
- Legal and Law Enforcement: Legal professionals and law enforcement agencies can utilize the algorithm to securely transfer images related to evidence, crime scenes, or confidential legal documents. This ensures the integrity and confidentiality of the images, maintaining their evidentiary value.

B. Suggestions for Further Improvements and Enhancements:

- Performance Optimization: Investigate techniques to optimize the algorithm's encryption and decryption speed without compromising security, ensuring efficient real-time image transfer over the internet.
- Scalability: Consider enhancing the algorithm to handle large-scale image datasets or high-resolution images commonly encountered in various applications, ensuring its practicality in real-world scenarios.
- Robustness against Advanced Attacks: Conduct research on enhancing the algorithm's resistance against advanced cryptographic attacks, including chosen-ciphertext attacks, side-channel attacks, or attacks exploiting implementation vulnerabilities.
- Adaptive Security: Explore the development of adaptive security mechanisms that can dynamically adjust the algorithm's security parameters based on the image content, transmission environment, or security requirements of different applications.

C. Identification of Future Research Directions in Image Encryption for Secure Internet Transfer:

- Multi-modal Encryption: Explore the integration of image encryption with other data types, such as audio or video, to develop multi-modal encryption techniques for secure multimedia transfer over the internet.
- Blockchain-based Solutions: Investigate the utilization of blockchain technology to enhance the security, integrity, and transparency of image transfer, ensuring traceability and accountability in distributed environments.
- Machine Learning and AI: Explore the integration of machine learning and artificial intelligence techniques to enhance image encryption algorithms, leveraging advancements in deep learning, adversarial learning, or generative models for improved security and robustness.
- Privacy-Preserving Techniques: Focus on the development of privacy-preserving image encryption techniques that protect sensitive information while still enabling image analysis and processing in privacy-sensitive applications, such as healthcare or surveillance.
- Post-Quantum Security: Investigate the resilience of image encryption algorithms against quantum computing-based attacks and explore the development of post-quantum encryption schemes suitable for image transfer.

IV. CONCLUSION

Undoubtedly, the cryptocurrency vision provides a secure way to send images over the Internet. Unlike most visual cryptography studies that focus on black and white images, this article uses V-AES and color matching. According to the color separation theory, each color of the color image can be decomposed into three primary colors: R, G, and B. In this paper, we propose a next-generation color sharing based on cryptography. In this scheme, the color image is encoded in two parts.

The hidden image has the same size as the original image and still retains visibility. In this study, image encryption and decryption are used by using V-AES algorithm to protect image data against unauthorized access. The implementation of the key symmetric AES algorithm is one of the best encryption and decryption models on the market. With the help of MATLAB coding, the realization of the V-AES algorithm for image encryption and decryption is synthesized and simulated. Original images can also be fully edited without interruption.

The results show that the algorithm has a wide range of security and can prevent the most common attacks such as brute force attack, password attack and plain text attack.

REFERENCES

[1] Chin chen Chang, Min Shian Hwang and Tung Shou Chen, “A new image encryption algorithm for image cryptosystems”, the journal of system and software 58(2001).

[2] H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 277-280, 2023.

[3] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing, pp. 483-492, 2020.

[4] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption", IEEE 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[5] Arpita Tiwari, Gori Shankar and Dr. Bharat Bhusan Jain, "Digital Image and Text Data Security Improvement Using The Combination of Stenography and Embedding Techniques", Design Engineering, no. 7, pp. 8592-8599, 2021.

[6] Himanshu Arora, Manish Kumar and Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, vol. 29, no. 8, pp. 6167-6177, 2020.

[7] Dr. Himanshu Arora, Gaurav Kumar Soni and Deepti Arora, "Analysis and Performance Overview of RSA Algorithm", International Journal of Emerging Technology and Advanced Engineering, vol. 8, no. 4, pp. 10-12, 2018.

[8] Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[9] M. Kumar, A. Soni, A. R. S. Shekhawat and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique", IEEE 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), pp. 1453-1457, 2022.

[10] S. Mishra, D. Singh, D. Pant and A. Rawat, "Secure Data Communication Using Information Hiding and Encryption Algorithms", IEEE 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), pp. 1448-1452, 2022.

[11] Trupti Patel, Rohit Srivastava, “A New Technique for Colour Share Generation using Visual Cryptography”, 2016.

[12] Vipin Singh, Manish Choubisa and Gaurav Kumar Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering & Management, vol. 83, pp. 30561-30565, May-June 2020.

[13] A. Agarwal, H. Arora, M. Mehra and D. Das, "Comparative Analysis of Image Security Using DCT LSB and XOR Techniques", IEEE 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 1131-1136, 2021.

[14] Vishal Pratap Singh, Manish Kumar and Himanshu Arora, "Enhanced image security technique with combination of ARNOLD transformation and RSA algorithm", International Journal of TEST engineering and management, vol. 83, pp. 30550-30560, May/June 2020.

[15] A. Tiwari, G. Shankar and B. B. Jain, "Comparative Analysis of Different Steganography Technique for Image Security", International Journal of Engineering Trends and Applications (IJETA), vol. 8, no. 2, Mar-Apr 2021.