IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10581

Image Encryption using Cryptography

Divakar HV[1], Lavanya MS [2], Nikhil Dhruva [3], Padmaja K[4], Pragna CP[5]

Assistant Professor, ISE, JIT, Bengaluru, India[1]

Student, ISE, JIT, Bengaluru, India[2-5]

Abstract: The paper focuses to enhance the security of digital images by implementing encryption through the Advanced Encryption Standard (AES) algorithm. A highly trusted and vastly employed encryption technology for securing image data both in transit and at rest is AES. The paper seems to employ dividing the digital data into data blocks and executing AES on each block. Encrypting the blocks forms the encrypted image file. To decrypt the image, the same encryption key used for encryption must be entered. Also, a significant improvement in terms of security, speed, and memory usage for different sizes and types of images is explored. The project aims to demonstrate the effectiveness of AES encryption in securing digital images and its potential for practical use in situations where image security is paramount.

Keywords: AES, Encrypt, Decrypt, k-n Share .

I. INTRODUCTION

AES is a widely used symmetric key encryption algorithm that is known for its security and efficiency. k-n Share is a symmetric key encryption method that uses a sequence of keys generated by a pseudorandom number generator to XOR with the image data. When used together, AES and k-n Share provide a high level of security for image encryption. The image data is first transformed into binary format and then divided into fixed-size blocks. The AES algorithm operates on each block, applying a series of mathematical transformations using a key of a certain length, which can be 128, 192, or 256 bits.

The resulting encrypted blocks are then XORed with a sequence of keys generated using the k-n Share technique. The size of the key sequence is equal to the size of the image data, and the sequence is divided into two parts, one for encryption and one for decryption. During decryption, the encrypted blocks are XORed with the decryption part of the key sequence, and then the AES algorithm is used to decrypt the resulting blocks. The original image data can then be reconstructed by reversing the process of transforming the binary data into image format. AES and k-n Share provide a secure and efficient method for encrypting and decrypting image data, ensuring confidentiality and accessibility only to authorized parties with the appropriate decryption key.

II. LITERATURE SURVEY

Image Encryption based on the RGB PIXEL Transposition and Shuffling 2013. This paper proposed a technique of transposition and reshaping the RGB values of the image in stages, which proved to be really effective [1].

Text and Image Encryption / Decryption Using Advanced Encryption Standard 2014. This paper implemented text and image encryption and decryption using AES. The data characteristics depend on its type. Therefore, same encryption text [2].

A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps 2015. This paper proposed an image encryption technique using DNA (Deoxyribonucleic acid) operations and chaotic maps. The intermediate result is DNA complemented with the help of a complement matrix produced by two 1D chaotic maps. Finally, the resultant matrix is permuted using 2D chaotic maps followed by DNA decoding to get the cipher image[3]

A Study of Encryption Algorithms AES, DES and RSA for Security 2013. This paper set up experiments for three encryption techniques: AES, DES and RSA algorithms and compared their performance on the basis of the algorithm [4].

Use of Symmetric Algorithm for Image Encryption 2014. This paper presented image encryption with DES algorithm which provides more security during the transmission. The proposed idea reproduces the original image with no information loss [5].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10581

III. METHODOLOGY

An image that is to be secretly transmitted should be selected and is displayed on window.
Password of string data, k and n shares values are to be specified.
Selected image then be encrypted using AES and it shows encrypted image.
Then split this encrypted image into 'n' shares using (k, n) secret sharing encryption algorithm.
'k' of 'n' shares are selected for merging.
If the k share selected is less than required then partial image is generated.
Once the shares are selected, then we overlap and combine these shares using (k, n) secret sharing decryption algorithm.
This will decrypt the merged image using AES algorithm.
The password that we generate earlier is used for AES decryption.
Wrong password leads to generation of noisy image which is not clear.

3.1 WORK FLOW DIAGRAM:

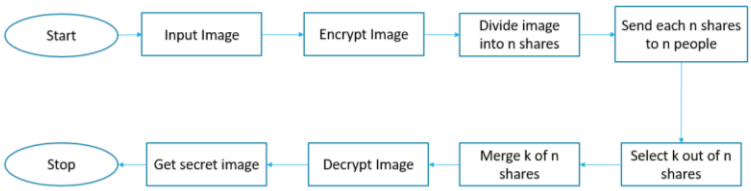

Fig : Work Flow Diagram

3.2 WORKING:

The AES algorithm has a block size of 128 bits. It supports three different key lengths of 128, 192 and 256 bits. AES replaced Data Encryption Standard and it is now used worldwide. In AES there is no Feistel Network as opposed to the previous standard DES. The cipher consists of rounds, where the number of rounds depends on the key length: 10 rounds for a 128-bit key, 12 rounds for 192 bits key, and 14 rounds for a 256-bit key. The whole algorithm operates on a 4 x 4 matrix of bytes. The first rounds consist of four distinct transformation functions: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. The final round contains three transformations. The Mix Columns function is not used in the final round. Each transformation takes one or more 4x4 matrices as input and produces a 4x4 matrix as output. Provided that all the four rounds are reversible, it is easy to prove that decryption does recover the plaintext.

- An image that is to be secretly transmitted should be selected and is displayed on window.
- Password of string data, k and n shares values are to be specified.
- Selected image then be encrypted using AES and it shows encrypted image.
- Then split this encrypted image into 'n' shares using (k, n) secret sharing encryption algorithm.
- 'k' of 'n' shares are selected for merging.
- If the k share selected is less than required then partial image is generated.
- Once the shares are selected, then we overlap and combine these shares using (k, n) secret sharing decryption algorithm.
- This will decrypt the merged image using AES algorithm.
- The password that we generate earlier is used for AES decryption.
- Wrong password leads to generation of noisy image which is not clear.

IV. RESULT

A test set of some photos was developed to test the suggested methods. A 256×256 grayscale image was used as the starting point. The share sizes match the dimensions of the original image. The results of embedding and extracting secret data from shares using proposed advanced encryption standards with K-N share technique are displayed in following.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10581

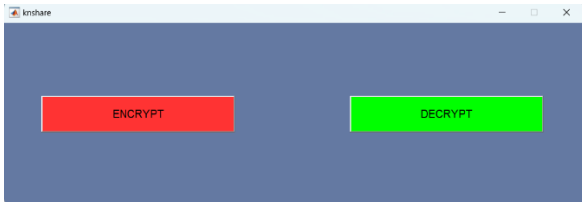

Fig. 4.1 KN-Share Main Screen

Execute command run K-N SHARE in MATLAB terminal. The K-N SHARE main Screen appears

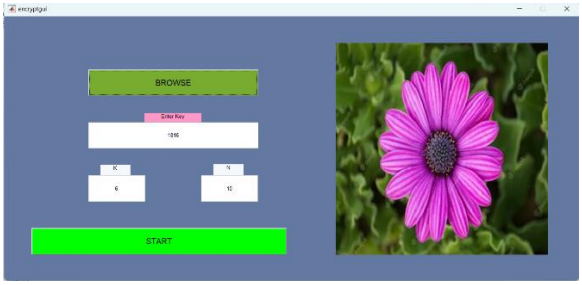

Fig. 4.2 Encryption Window

Click on ENCRYPT button to open the encryption window

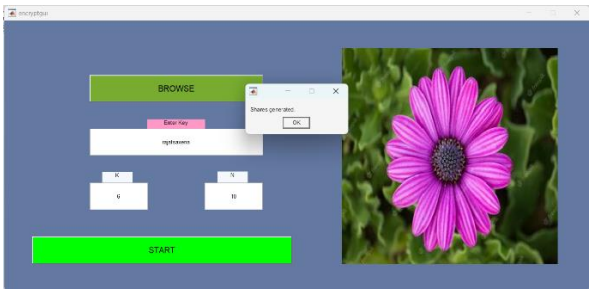

Fig. 4.3 Share generation message in encryption window

Click on BROWSE button to open the File Selector.Select the file.Now proceed on filling the value of K,N and enter a secure password to encrypt the image.After the process completes,the user is presented with a “Shares Genrated” message.

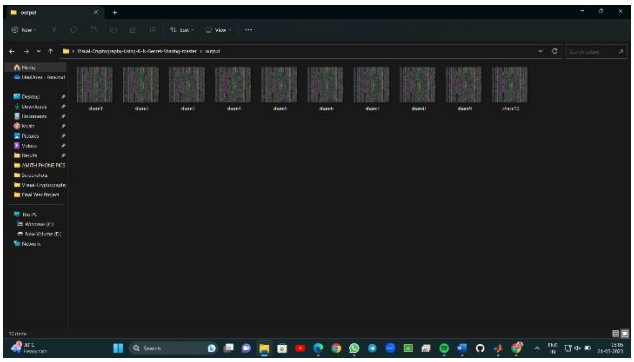

Fig. 4.4 Generated Shares

These are the shares generated

.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10581

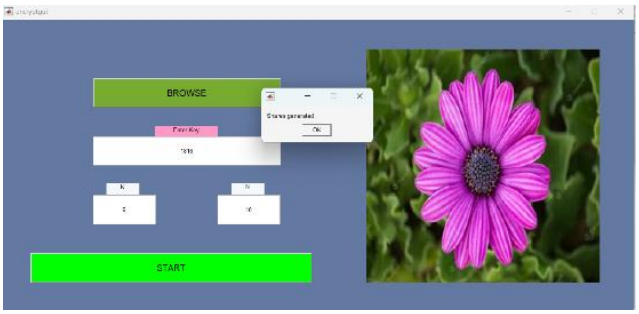

Fig. 4.5 Decryption Window

After Sometime,the unencrypted image appears on the right.It is same as the original image.After successful completion the message appears"Image Successfully Decrypted".

V. CONCLUSION

In today's digital era, the security of images has become increasingly crucial due to the rapid growth in communication and data exchange. With the widespread use of technology, it is essential to ensure that images are protected from unauthorized access and potential breaches. Traditional image encryption methods have limitations and provide only a minimal level of security.

To address this issue, a new approach to image encryption has been proposed, aiming to enhance both efficiency and security while minimizing computational requirements. This novel image encryption technique employs advanced algorithms that offer a significantly higher level of protection. By leveraging cutting-edge cryptographic techniques and sophisticated encryption algorithms, this method ensures that image data remains secure and confidential.

The application of this encryption technique has undergone extensive simulations and testing to evaluate its performance and effectiveness. The results have demonstrated that this approach provides numerous advantages over other commonly used methods for image encryption. It has proven to be highly efficient and offers a high degree of security, particularly in public networks and communication channels.

One of the significant advantages of this advanced image encryption method is its reliance on the RSA algorithm. RSA (Rivest-Shamir-Adleman) is a widely recognized and trusted encryption algorithm that provides strong security guarantees. The encryption process involves generating public and private key pairs, where the public key is used for encryption, and the private key is used for decryption. This asymmetric encryption scheme ensures that only authorized parties with the private key can decrypt and access the encrypted image data.

Moreover, this encryption technique employs additional measures to enhance security. It includes techniques such as key stretching, which increases the complexity of the encryption process, making it harder for attackers to crack the encryption key. Additionally, it incorporates randomization and padding mechanisms to further strengthen the security of the encrypted images.

In the digital world, where communication is rapidly expanding, the security of images plays a pivotal role. The ability to securely encrypt and decrypt images ensures that sensitive image files can be shared with utmost security. Whether it is transmitting images over the internet, storing them in the cloud, or transferring them via various communication channels, employing robust image encryption techniques is paramount.

Furthermore, encryption serves as a safeguard for devices that are at risk of being lost or stolen. By encrypting the images stored on these devices, even if they fall into the wrong hands, the data remains protected and inaccessible without the appropriate decryption key. This not only safeguards sensitive images but also protects the privacy and confidentiality of individuals and organizations.

The advanced image encryption methods available today offer several key advantages. They provide a higher level of security, ensuring that images are protected from unauthorized access and potential breaches. These methods employ sophisticated algorithms and techniques that are designed to resist various cryptographic attacks, ensuring the confidentiality and integrity of the encrypted image data.

DOI: 10.17148/IARJSET.2023.10581

Additionally, these encryption techniques are efficient and computationally optimized, minimizing the computational requirements and processing time associated with encryption and decryption operations. This makes them suitable for real-time applications and systems where efficiency and performance are critical.

The application of advanced image encryption techniques is not limited to specific industries or domains. It is a universal solution that can benefit various sectors, including healthcare, finance, e-commerce, and government agencies. These encryption methods provide a robust security framework, ensuring that images containing sensitive information, such as medical records, financial data, or classified documents, remain protected and secure.

In conclusion, the advanced image encryption methods available today provide a crucial solution for maintaining the confidentiality and integrity of images. They offer enhanced security measures, allowing users to securely share images and protect their devices from potential threats in the digital realm. By leveraging sophisticated algorithms and techniques, these encryption methods ensure that sensitive image data remains confidential, even in the face of sophisticated attacks. As the digital landscape continues to evolve, the importance of robust image encryption techniques cannot be overstated.

REFERENCES

[1] Forouzan BA. Cryptography & network security, 1st edn. TMH
[2] Kahate A. Cryptography and network security, 2nd edn. TMH
[3] Al Sabti KDM, Hashim HR (2016) A new approach for image encryption in the modified RSA cryptosystem using MATLAB. Glob J Pure Appl Math 12(4). ISSN 0973-1768
[4] Sethi PC, Behera PK (2015)Methods of network security and improving the quality of service—a survey. Int J Adv Res Comput Sci Softw Eng 5(7):1098–1106
[5] Sethi PC, Behera PK (2016) RSA cryptography algorithm using linear congruence class. Int J Adv Res 4(5):1335–1347
[6] Sheu T-F, Huang N-F, Lee H-P (2010) In-depth packet inspection using a hierarchical pattern matching algorithm. IEEE Trans Dependable Secure Comput 7(2)
[7] Durairaj M, Muthuramalingam K (2018) A new authentication scheme with elliptical curve cryptography for internet of things (IoT) environments. Int J Eng Technol 7(2.26):119–124. https://doi.org/10.14419/ijet.v7i2.26.14364
[8] Sethi PC, Behera PK (2017) Network traffic management using dynamic bandwidth on demand. Int J Comp Sci Inf Secur (IJCSIS) 15(6):369–375
[9] Kumar, M. Arun, and K. Jhon Singh, "Novel Secure Technique using Visual Cryptography and Advance AES for images.", International Journal of Knowledge Management and e-learning, Vol. 3, No. 1, pp. 29-34, 2011.
[10] Nikita, Ranjit Kaur, "A Survey on Secret Key Encryption Techniques", Impact: International Journal of Research in Engineering & Technology IMPACT: IJRET, May, 2014. 2016 2nd International Conference on Next Generation Computing Technologies (NGCT-2016) Dehradun, India 14-16 October 2016 812
[11] Chang, C. C. and Yu. T. X., "Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice", Tokyo, Japan, Nov. 2002.
[12] M. Naor and A. Shamir, Visual cryptography. "Advances in Cryptology" EUROCRYPT '94, 1995 [6]. C. Chang, C. Tsai, and T. Chen, "A new scheme for sharing secret color images in computer network"., International Conference on Parallel and Distributed Systems, July 2000.
[13] E. Verheul and H. V. Tilborg., "Constructions and properties of k out of n visual secret sharing schemes. Designs", Codes and Cryptography, 1997.
[14] C. Yang and C. Laih., "New colored visual secret sharing schemes. Designs", Codes and Cryptography, 2000.
[15] Kulvinder Kaur and Vineeta Khemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption", Advance Computing Conference (IACC), Feb, 2013
[16] Orr Dunkelman, Nathan Keller⋆, and Adi Shamir, "Improved Single-Key Attacks on 8-round AES-192 and AES-256", ASIACRYPT, LNCS, 2010.
[17] Alex Biryukov, Dmitry Khovratovich, Ivica Nikolić, "Distinguisher and Related-Key Attack on the Full AES-256", Advances in Cryptology - CRYPTO 2009
[18] Joan DAEMEN, Vincent RIJMEN, "On The Related-Key Attacks Against AES", Proceedings of The Romanian Academy, Series A, 2012
[19] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir, "Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds", Cryptology ePrint Archive, 2009
[20] Andrey Bogdanov⋆, Dmitry Khovratovich, and Christian Rechberger⋆, Biclique Cryptanalysis of the AES-192 and AES-256, "International Conference on the Theory and Application of Cryptology and Information Security", 2009.

DOI: 10.17148/IARJSET.2023.10581

[21] S. Parker., L. O. Chua., "Chaos: a tutorial for engineers. Proceedings of the IEEE", vol. 75, no. 8, pp. 982–1008, 1995

[22] W.Wu .,N. F. Rulkov., "Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I Fundamental Theory and Applications", vol. 40, no. 10, pp. 707–721, 1993

[23] Chin-Chen Changa, Min-Shian Hwangb, Tung-Shou Chenc, "A new encryption algorithm for image cryptosystems", 2000

[24] Y.-Q. Zhang, X.-Y. Wang "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation", 2014.

[25] Y.-Q. Zhang, X.-Y. Wang "A new image encryption algorithm based on non-adjacent coupled map lattices", 2015.

[26] H. Liu, X. Wang "Color image encryption based on one-time keys and robust chaotic maps" 2010

