A Novel Method For Data Security Using Coverless Image Steganography Using AES

Arjun Das[1]
B-tech Student
Computer Science &Engineering
Mangalam College Of Engineering

Harsha Wilson[2]
B-tech Student
Computer Science &Engineering
Mangalam College Of Engineering

Sophiya Sunny[3]
B-tech Student
Computer Science &Engineering
Mangalam College Of Engineering

Mr Sanoj C Chacko [4]
Assisitant Professor
Computer Science &Engineering
Mangalam College Of Engineering

***Abstract*— We need safe solutions to protect our data as data threats grow. Techniques like cryptography and cryptography can aid in preventing security threats from hostile actors. Data security can be increased by combining cryptography and cryptographic recording, and there are currently systems that do this. However, these systems frequently employ concealed hiding methods. To further strengthen data security in our proposed work, we advocate adopting encryption algorithms in conjunction with non-masking picture concealment approaches. Data encryption in our system uses a 128-bit version of the AES symmetric technique. We have opted for non-masking cloaking because image analysis technologies are particularly sensitive to conventional cloaking. In unwrapped photo steganography, hidden messages are inserted into a cover image. The combination of encryption and non-masking imaging is what we aim to do in order to increase data security. The unique idea of unwrapped image concealment, developed by A.H.S. Saad and colleagues, is used in the suggested system as an image storage technique with the highest payload capacity when compared to non-covered image storage algorithms.**

Keywords—Information Security, Cryptography, Steganography, Advanced Encryption Standard (AES),Symmetric Cryptography, Coverless Image Steganography.

I. INTRODUCTION

Data security is a critical problem in the current climate, when data breaches and cyber-attacks are occurring more regularly. A hybrid approach that combines the Advanced Encryption Standard (AES) and coverless image steganography is an effective data protection technique. Steganography is a method of concealing information in an image in a way that the naked eye cannot see it. A more sophisticated form of steganography calledcoverless image steganography does not need a cover image toconceal information. Instead, it conceals information using thefeatures of the image file format itself. Data is securely encrypted using the popular encryption method AES. We can offer a two-layered solution to data security by fusing coverless image steganography with AES. The data is first encrypted with AES, making sure that even if it is intercepted, it cannot be decoded without the decryption key Secondly, to make it even more challenging to detect and intercept, the encrypted data is cloaked inside an image using coverless image steganography. Data security benefits from the combined use of coverless image steganography with AES are numerous. Because the data is encrypted using a powerful encryption algorithm and concealed within an image, it offers ahigh level of security. As a result, it is challenging for hackers to intercept and interpret the data. Additionally, coverless image steganography adds an extra layer of security because there is no obvious sign of the concealed data, making it challenging to find. A method of concealing information within a picture without changing its look is called coverless image steganography. With coverless image steganography, information can be concealed without a cover image, in contrast to traditional steganography. Instead, it conceals information using the features of the image file format itself. Data is securely encrypted using the Advanced Encryption Standard (AES), a popular encryption method. Because it uses symmetric keys, the same key is used for both encryption and decryption. Data security can be effectively solved with the use of coverless image steganography and AES.

Data encryption: Data is first encrypted with the AES method. To guarantee that only people with permission can decrypt and access the data, the encryption key must be kept secret.Steganography embedding Next, using coverless image steganography, the encrypted data is incorporated into theimage . The image can be any image file format, such as JPEG or PNG. The embedded data is distributed across the image pixels, making it difficult to detect.Data extraction : The encrypted data is initially taken from the image utilizing coverless image steganography techniques in order to extract the data. Afterward, the data that was extractedis decrypted using the original encryption key. It is crucial to remember that the security of the hybrid solution also depends on how the algorithms are applied and how strong the encryption key is. To maintain the highest level of data security, it is crucial to utilize a strong encryption key and accurately apply the algorithms.

II. RELATED WORK

Two popular encryption methods in data security are AES (Advanced Encryption Standard) and DES (Data Encryption Standard). Here are some related works on AESand DES data security.

[1]. By A. Al-Masri and M. Al-Qutayri (2015), "A Comparative Analysis of AES and DES Encryption Algorithms": In this study, the security and speed of encryption using the AES and DES encryption algorithms are compared. According to the authors, AES is quicker and more secure than DES.

[2]. In their paper "DES vs AES Encryption Performance Comparison on CPU and GPU" published in 2018: In this study, the efficiency of the DES and AES encryption algorithms on CPU and GPU platforms is compared. The authors come to the conclusion that on both platforms, AES is faster and more effective than DES.

[3]. "S. M. Naqvi and A. M. Abbas' "A New Image Encryption Algorithm B d on AES and DES" (019): In this paper, a brand-new image encryption technique built on DES and AES is proposed. The authors demonstrate that the suggested technique offers greater security and performance than the ones currently used for image encryption.

[4]. "Enhancing the Security of DES and AES Algorithms using Chaos and Hashing Functions" by S. M. Naqvi and A. M. Abbas (2019): Using chaos and hashing functions, this study suggests a technique to increase the security of the DES and AES encryption algorithms. The authors present evidence to support their claim that the suggested approach offers more security than the original algorithms.

[5]. S. Singh and A. K. Sharma's article "A Comparative Analysis of AES and DES Encryption Techniques for Securing Patient's Data in Healthcare Information Systems" (2020): In order to secure patient data in healthcare information systems, this article evaluates the effectiveness of the AES and DES encryption algorithms. The authors come to the conclusion that AES is more effective and secure than DES for encrypting healthcare data.

III. METHODOLOGY

A. Proposed System

Standard for Advanced Encryption Asymmetric block cypher Rijndael, developed by Belgian researchers Joan Daemen and Vincent Rijmen and afterwards known as AES,was first suggested in 1988.

The Advanced Encryption Standard (AES) was created to address the drawbacks of prior symmetric algorithms like DES and Triple DES and offers more security. AES is used more frequently since it offers high security and takes less time to encrypt and decrypt data. AES uses a block of 128 bits as its input and generates a block of 128 bits as its output after performing encryption or decryption using a changeable key length of 128, 192, or 256 bits. The algorithm's round count is influenced by the length of the keyThe proposed system utilizes the AES-128 variant for its cryptography part, which involves 10 rounds of transformations using four types of inverse operations: Substitution,Permutation, Mixing, and Key-adding. To execute these transformations, the 128-bit input is organized into a 4x4 matrix of 16 bytes, known as the state. During the Substitution process, each byte in the state undergoes a replacement with a different byte from the transformation table, also known as the lookup table. AES-128 uses two substitution transformations, namely Sub Bytes and In v SubBytes.

SubBytes: This particular operation is employed during the encryption process. It involves converting a byte into two hexadecimal digits. In the substitution table, the row number corresponds to the left digit of the hexadecimal number, and the column number represents the right digit. The value found at this intersection is then placed in the same location of the output matrix as the input matrix.In v SubBytes: It is the inverse of SubBytes. This transformation used in the decryptionsite. Each byte of the matrix is substituted with the inverse s- box table to get the output matrix.Permutation: In this, the bytes are permuted. The two permutation transformations used in AES are ShiftRows and InvShiftRows.

ShiftRows: The encryption site employs this transformation. The row is moved to the left in this alteration. The number of shifts matches the number of rows in Table 1 exactly. In general, a row's position in the output matrix is shifted by 'n' bytes if the row is 'n'.ShiftRows: The encryption site employs this transformation. The row is moved to the left in this alteration. The number of shifts matches the number of rows in Table 1 exactly. In general, a row is moved by 'n' bytes if the row is 'n'.

B. Algorithm

1. Read the image content and convert to byte using base 64.
2. Using the cipher key, the set of round key is generated.
3. Filled the state array with data .
4. Initial round key is added with the starting state array.
5. Perform all nine round.
6. Perform the final round of AES encryption.
7. Encrypted message is obtained in the final step.

C. System Architecture

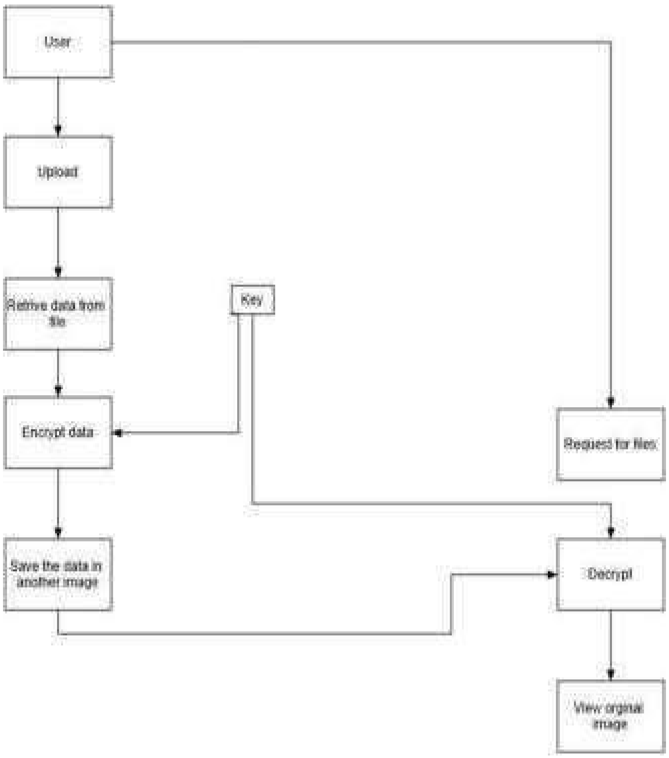
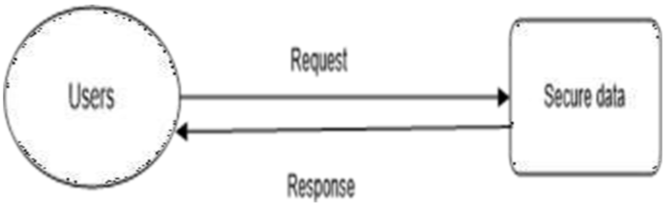
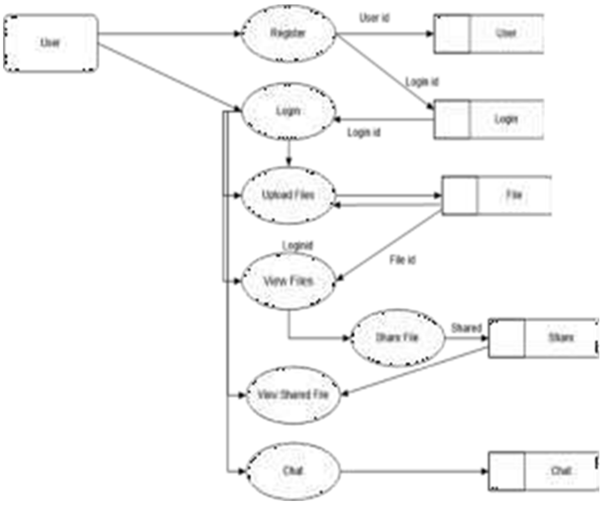


Fig.1.system architecture

D. DFD LEVEL 0



DFD LEVEL 1



E. Workflow diagram

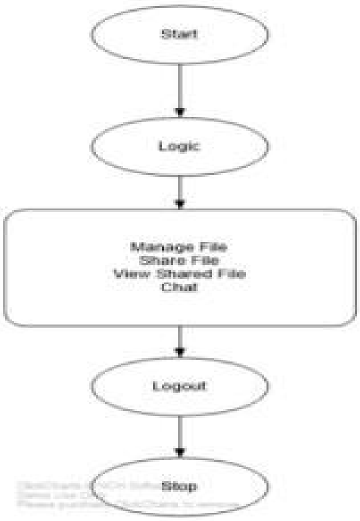


Fig.2.Workflow diagram

IV. EXPERIMENT AND RESULT

The experiment and result are demonstrating the potential of data security using coverless image steganography. The system use AES and coverless image stenography as cryptography and steganographic technique respectively. This system result in cost effective solution for secure data transfer.

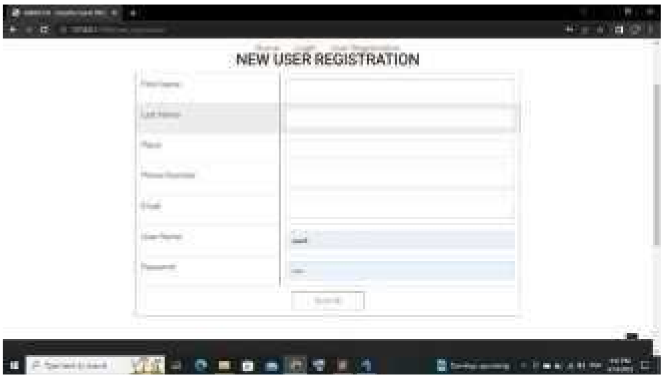


Fig 1: SNAPSHOT OF USER REGISTRATION

Fig 1 represent the first phase of proposed system. As the first stage a platform called slime is initiated where a fresh user gets his first registration process. Here the user must provide his personal details and must create a login id and a password. This login id and password is pre processed in next stages.

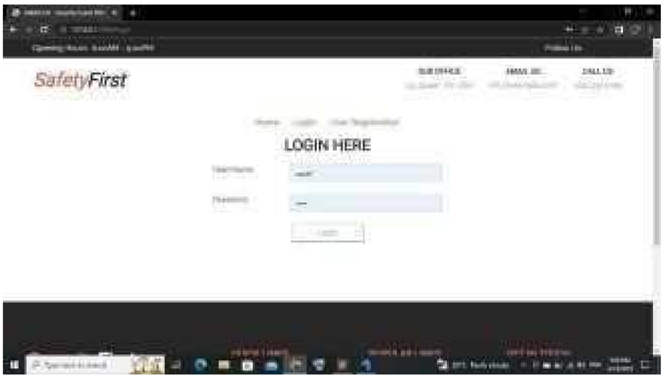


Fig 2: SNAPSHOT OF USER LOGIN

Fig 2 represent the 2 nd phase of the interface where user must log in to the server using login id and a password created. The user name and password are cross matched in this stage. If the user is valid only the program will allow to proceed. The Authorized persons can view the registerd details of user through sqlyog community.

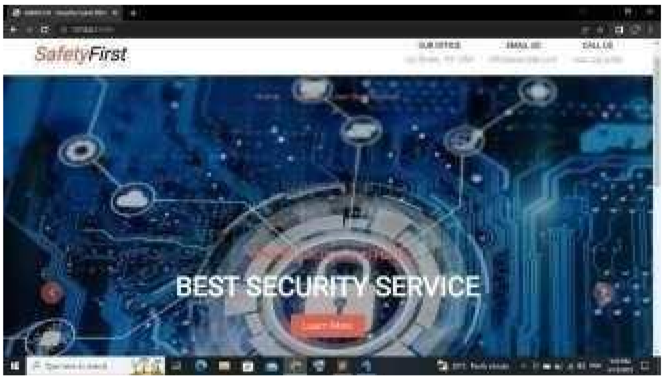


Fig 3: SNAPSHOT OF USER MODULE

After the login process completed the user data is registered to the server. Then returns to slime platform to transfer the user data codes to server database. Then runs the code main.py when main program processed press cntrl+b to go for the next stage. A pop up panel appears with a redirection link.

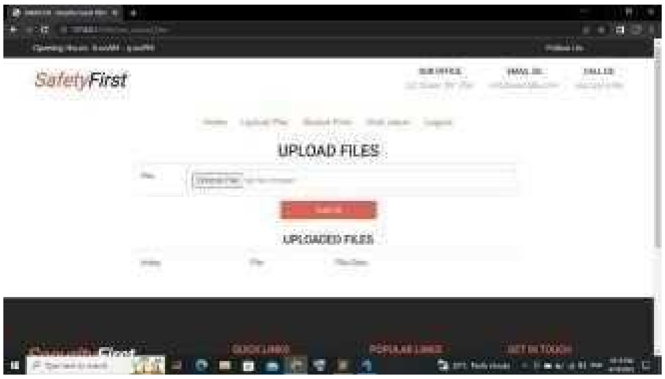


Fig 4: SNAPSHOT OF USER FILE UPLOAD

Fig 4 represent final stage where the user gets an interphase for uploading his files and datas to server for encrytion. Final out put is displayed on the interface. Files are encrypted and store to server in this stage. After encryption files can be viewed by user only.

V. CONCLUSION

The preprocessed for data security which uses coverless image stegnography and cryptography. The present systems have many disadvantages that they use traditional image stegnography which are weak to resist modern cyber attacks. But our work focus on coverless image encryption. AES algorithms is used in cryptography part for encryption for 128 -bit plaintext using 128- bit key and then the resultant encrypted message is covered into bitstreams. AES Is more often to use as this algorithm consumes less encryption and description time. By using these techniques system becomes more powerfull than traditional softwares. Thus we can replace our system agnist traditional softwares.

VI .REFERENCES

[1]. Dhamija, Ankit & dhaka, vijay. (2015). A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration. 10.1109/ICGCIoT.2015.7380486.

[2]. Ali Ahmed and Abdelmotalib Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations," IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.5, May 2020.

[3]. F. Anwar, E. H. Rachmawanto, C. Atika Sari and D. R. Ignatius Moses Setiadi, "StegoCrypt Scheme using LSB-AES Base64," 2019 International Conference on Information and Communications Technology (ICOIACT), 2019, pp.85-90, doi:10.1109/ICOIACT46704.2019.8938567.

[4]. Joshi, Kamaldeep & Yadav, Rajkumar. (2015). A new LSB-S image steganography method blend with Cryptography for secret communication. 86-90. 10.1109/ICIIP.2015.7414745.

[5] S. Aiswarya and R. Gomathi, "Review On Cryptography and Steganography Techniques in Video," 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2018, pp. 1-4, doi: 10.1109/ICCIC.2018.8782409.

[6]. Kusuma, Edi & Sari, Atika & Rachmawanto,Eko & Setiadi, De Rosal Ignatius Moses. (2018). ACombination of Inverted LSB, RSA, and ArnoldTransformation to get Secure and Imperceptible Image Steganography. Journal of ICT Researchand Applications.12.103.10.5614/itbj.ict.res.appl.2018. 12.2.1.

[7]. Biswas, Sushanta & Sarkar, Debasree & Sarkar, Partha & Nag, Amitava. (2011). A Novel Technique for Image Steganography Based on DWT and Huffman Encoding. International Journal of Computer Science and Security.

[8]. Gupta, Rupesh & Singh, Tanu. (2015). New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters. Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014. 475-479. 10.1109/IC3I.2014.7019643.

[9]. Rajkumar, & Rishi, Rahul & Batra, Sudhir.(2010). A New Steganography Method for GrayLevel Images using Parity Checker. International Journal of Computer Applications. 11. 10.5120/1627-2188.