WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Advance Secure Information Exchange

Sabyasachi Banerjee[1], Parreddy Divya Shanmukh Reddy[2], Shaik Jiyaull Haq Ali[3], Mr. N. Siva Kumar[4]

[1,2,3]Department of CSE, Aditya Engineering College, Surampalem, A.P., India

[4]M. Tech, (Ph.D), Sr. Assistant Professor, Department of CSE, Aditya Engineering College, Surampalem, A.P., India

ABSTRACT:

Nowadays, information has become one of the most important vulnerabilities for a person in their regular life, due to the importance of their data. In that context, Social networking keeps track of users' private data as well as additional data, turning it into a daily activity tracker that reveals crucial details about the user. Because each tool can only give basic information on a particular application and activity, there aren't many tools accessible to utilise for this intent as a result of all the data that has been acquired. Consequently, the current study suggests a tool that enables users to upload the data and inject a payload that can be securely exchanged or transferred through any social media. Additionally, an instance is used to demonstrate what the approach works, demonstrating the tool's functionality and demonstrating how to utilise it which encryption and decryption must apply for the security of the data.

1. INTRODUCTION

The developing utilization of the Web needs to take consideration while we send and get individual data in a solid way. We get to see a lot of vulnerabilities in social media platforms. There are more than millions of cyber attacks across the world. Obviously the cyber attacks could not be stopped, people get away easily. Therefore we can focus on making our applications more secure. This Product focuses on the Encryption and Decryption of the data. This isn't any ordinary Product, This is a carefully engineered product which focuses on the secure information exchange between the users irrespective of the medium of exchange they use. Compared to the present version of the technology, The technology used in this product is advanced. We have fixed major issues and made it better and more convenient for people to encrypt and decrypt data and exchange data online via any social media application like Facebook, Instagram moving them ahead by providing safe and secure data transfer to the users across the internet. We'll utilize Steganography which is the method of concealing privileged information inside a normal, non-mystery, document or message to keep away from identification. The restricted information is then extricated at its objective. The utilization of steganography can be joined with encryption as an additional step for stowing away or safeguarding information. At the same time we'll be using a special algorithm which will be using a number of patterned encoding and patterned decoding and a Hashing which will make hacking impossible. This is going to make the world a safe place for people to exchange their information

2. LITERATURE REVIEW

Visual Cryptography:

Steganography is the craft of concealing restricted information in a medium while visual-cryptography is a cryptographic strategy where a full picture is encoded.The security of image steganography relies upon the mystery key set which is utilized for embedding the mystery picture. On the off chance that the secret key is uncovered, the mystery image can be recovered. To tackle this security issue we propose another sort of steganography strategy utilizing visual cryptography. In this method, text and image are utilized as a mysterious message and image for the cover object. 24-bit RGB tone images are utilized as both mystery and cover images. In this method, we use another picture to be specific share1 which changes over a mystery picture to an entirely unexpected picture called share2 picture. Regularly, knowing the extraction technique, individuals can recover the secret message without any problem. A pseudorandomly created picture is utilized as a key for visual encryption and this guarantees the additional layer o f security.

LSB and discrete wavelet transform technique:

Steganography is ordered among the first strategies utilized in information security to cover and shield classified messages in the information sent. Security, particularly information security, is a significant imperative in this day and age thus Steganography has extraordinary importance. The strategy manages understanding and execution of steganography on various pictures utilizing two distinct procedures: Least Huge Piece method(secret picture is covered up utilizing the pieces essentially critical level of the cover picture) and Discrete Wavelet Change method(secret picture is concealed by alteration of the wavelet coefficients of cover picture). The picture to be communicated covertly is both encoded and decoded utilizing these strategies and a definite investigation of the resultant pictures is performed utilizing different picture boundaries.

Symptoms Based Disease Prediction Using Machine Learning Techniques:

Computer Aided Diagnosis (CAD) is being evolved quickly such that the medical analysis is also being done by the computer but this require correct results. Several CAD applications has been created but most of them are deceptive such that there may be failures and the medial therapies can be different for different diseases but because of the mistake in prediction they may be interchanged. The body organs cannot be determined by a simple equation. Hence, the Machine Learning is introduced here to recognise the patterns and to learn continuously based on the previous disease data. This requires training a system which can be achieved in Machine Learning and hence the disease can be predicted correctly by using the medical analysis data by using algorithms and some decision-making process.

Using LSB and AES algorithm:

Information shared through this medium is a very sensitive to the users. Hence it is highly needed to secure the message from the intruders. This paper proposed an android based secured system named Steg! developed by combining the cryptography and steganography. Here the algorithm used for cryptography is Advanced Encryption Standard (AES) and Least Significant Bit is used for the steganography. This hybrid approach increases the level of secretion of information from unauthorized the access by encrypting the message and hiding into the image. The application helps the user to hide/unhide the text to/from the image.

Using Discrete Wavelet Transform and Singular Value Decomposition:

This method presents a picture procedure Discrete Wavelet Change and Solitary Worth Disintegration for picture steganography. Text record is being utilized and convert into a picture as watermark and insert watermarks into the cover picture. Execution is being assessed and contrasted this technique and different strategies like Least Critical Piece, Discrete Cosine Change, and Discrete Wavelet Change utilizing Pinnacle Signal Commotion Proportion and Mean Squared Blunder. The aftereffect of this analysis showed that consolidate of Discrete Wavelet Change and Solitary Worth Deterioration execution is superior to the Most un-Critical Piece, Discrete Cosine Change, and Discrete Wavelet Change. The consequence of Pinnacle Signal Clamor Proportion acquired from Discrete Wavelet Change and Solitary Worth Deterioration technique is 57.0519 and 56.9520 while the aftereffect of Mean Squared Mistake is 0.1282 and 0.1311.

3. METHODOLOGY

First we will be taking the password and payload and we will be converting both of them into string .After that we will be concatinating both of them .Then the result(concatinated output) will be encrypted with a key .Then the result what we got after encryption will be converted into string .In order to make it suitable for encoding we will be converting the string to bytes. Now we will take the cover file and make it suitable for manipulation .The bytes output will be placed in the alpha channel of the image. In decryption methodology , first of all we will process the file.After that we will extract the output from the alpha channel of the image.Then we will decode it.We will take the encypted message and decrypt it using the same key since we are using symmetric key cryptography.Then extracted message will be splitted and the password will be extracted.

Disadvantages:

1.Lack of robust encryption: If the steganography system doesn't incorporate strong encryption techniques, it can be susceptible to various attacks, making it easier for adversaries to uncover the hidden information.

2. Detection risk: Advances in steganalysis, the process of detecting hidden data in steganographic systems, have made it possible to uncover many steganographic techniques. If the system is not regularly updated to stay ahead of steganalysis methods, it may be vulnerable to detection.

3.User error: Since steganography often involves hiding information within seemingly innocuous files, there is a risk of accidental deletion, modification, or sharing of the carrier file, which could compromise the hidden data.

Proposed system and Advantages

- In the proposed system, there will be an interface for two components .One component is the encrypt component. The encrypt component is responsible for taking the initial password, the cover image and the payload or the secret text. Then there will be a button .On pressing it will encrypt the information and results in the creation of the final payload. Another component is the decrypt. This component will take the final payload as the input as well as the password .There will be a button for decrypt. If the password is wrong in total three chances will be given. After that the file will be deleted automatically. Also if the password is right ,then the secret message will be displayed and the file will be deleted for security reasons.
- One major advantage of it is that the final output file can be send through any social media.The intresting fact is that the social media does not effect the secret message embedded in it. Also apart from social media it can be send through storage devices such as USB.
- .Another advantage of it is that brute force is not possible because only three chances are given. If someone enters wrong password three times then the file will be deleted automaticallytrained and tested thoroughly. Finally, the result will be displayed in webpage.
- On entering the correct password also, the secret message will be displayed but the file will be deleted for security reasons.

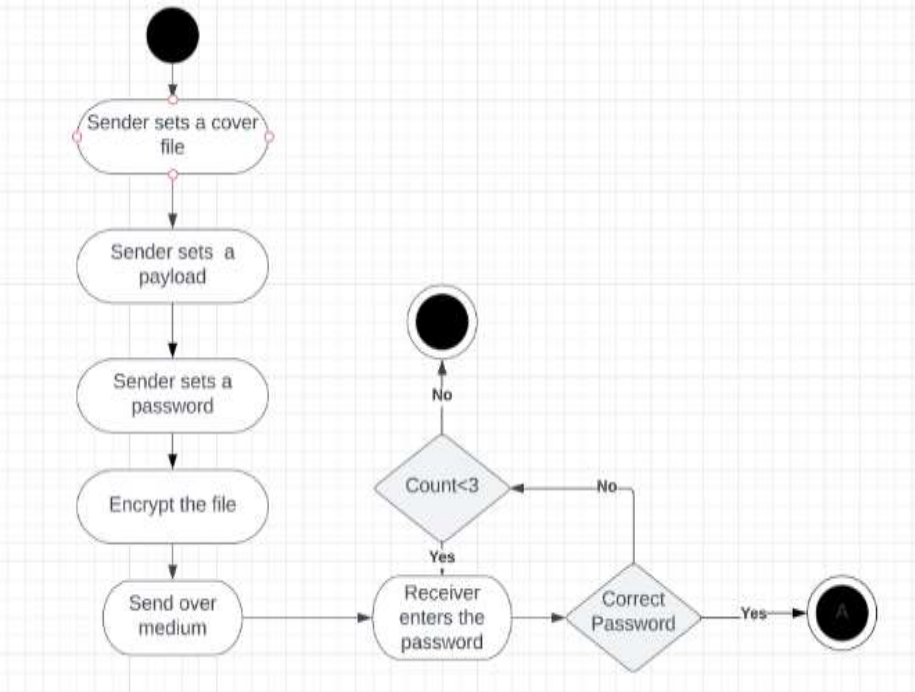

Fig.1: System architecture

MODULES:

We created the following modules for this project.

1.There will be two components of the desktop app. One is the encrypt part where we will be taking the initial password, payload or the secret message, the cover file and encrypt it.

2.Another component is the decrypt part, where we will be taking the final payload and the password and decrypt it

3.The system we will be responsible for calling the corresponding backend encrypt/decrypt backend function.

4. IMPLEMENTATION

The implementation of the project is based on frontend and backend .For Frontend we are using Angular Framework.

In the backend we are using tauri framework with rust as a backend language .Tauri is a cutting edge system that permits you to configuration, create and construct cross-stage applications utilizing recognizable web innovations like HTML, CSS, and JavaScript on the frontend, while exploiting the strong Rust programming language on the backend. Tauri is structure freethinker .Now tauri is used for converting web applications to desktop applications .We are having two sections or modules in the application we can say .One is the encode section and other is the decode section .In encode section we will be taking some inputs from the user such as the cover image which will be shown as the final output, the initial password and the secret text/the payload .Now we will be having an encode option where we will be using the custom encryption algorithm .The encryption algorithm is the heart of the application.

Encryption Algorithm

First we will be taking the password and payload and we will be converting both of them into string .After that we will be concatinating both of them .Then the result(concatinated output) will be encrypted with a key .Then the result what we got after encryption will be converted into string .In order to make it suitable for encoding we will be converting the string to bytes. Now we will take the cover file and make it suitable for manipulation .The bytes output will be placed in the alpha channel of the image.

Decryption Algorithm

In decryption algorithm, first of all we will process the file.After that we will extract the output from the alpha channel of the image.Then we will decode it.We will take the encypted message and decrypt it using the same key since we are using symmetric key cryptography.Then extracted message will be splitted and the password will be extracted.

5. EXPERIMENTAL RESULTS

Fig.2: Encode section of the application

Fig.3: Choose a cover image.

Fig.4: Once the cover image is chosen,it will get displayed in the choose file section.

Fig.5: After the cover image we will set a password.

Fig.6: We need to provide the payload in the payload section

Fig.7: This is the decode section of the application

Fig.8: In the decode section we need to provide the encrypted file to get processed.

Fig.9: Once the file is chosen,it will get displayed

Fig.10: If we provide wrong password in the password area,it will show the message as “Wrong password” along with number of left chances.

Fig.11: If we provide the right password then the secret message will be displayed and the file will be deleted

6. CONCLUSION

Though quite a few of most common visual steganographic approaches were covered in this document, it is clear that there are many different methods for concealing information in images. Each of the main formats for images has a unique way of evading messages, each having different strengths and weaknesses. Where one method falls short on payload capacity, the alternative technique falls short on robustness. The patchwork technique, for instance, is quite resistant versus the majority of assaults but can only conceal just a small quantity of data.

This is compensated for by the least significant bit in both BMPs, but both techniques produce suspicious documents that raise the likelihood of being discovered when a warden is present.

The strategy advocated in this research makes use of picture steganography, a fresh method of steganography. The sensitive data is contained into the cover file image that the programme produces as a stego picture.

In this project, the Least Significant method was used to construct the software since it is quicker, more dependable, and has a modest compression rate in contrast with other algorithms.

REFERENCES

[1] Rosziati Ibrahim and Teoh Suk Kuan, Steganography Imaging System (SIS): Hiding Secret Message inside an Image.

[2] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography

[3] Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications, 1(7), pp. 361-366, (2016).

[4] Pandit, A. S., Khope, S. R., & Student, F. Review on Image Steganography. International Journal of Engineering Science, 6115, (2016).

[5] Thenmozhi, M. J., &Menakadevi, T. A New Secure Image Steganography Using Lsb And Spiht Based Compression Method. International Journal of Engineering, 16(17), (2016).

[6] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, “Novel Approach for Cover File of Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.”, Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-508

[7] Hidden Data in PE-File with in Unused Area One”, International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198, p.p 669-678.

[8] Yung-Chen Chou, Hsin-Chi Liao "A Webpage Data Hiding Method by Using Tag and CSS Attribute Setting",IEEE-2014

[9] Babita Ahuja,Anuradha, Dimple Juneja "Dynamic Query Processing forHidden Web Data Extraction",IEEE-2015

[10] Chun-Juan Ouyang, Chang-Xin Liu, Ming Leng, Huan Liu, International journal of pattern Recognition and Artificial Intelligence, vol. 31,no. 01(2017)

[11] P. Mohamed Fathimal, P. Arockia Jansi Rani international journal of image and Graphics, vol. 16, No. 02(2016)

[12] Grībermans, D., Jeršovs, A., Rusakovs, P.: Development of requirements specification for steganographic systems. Appl. Comput. Syst. 20(1), 40–48 (2016).

[13] Snasel V, Kromer P, Safarik J and Platos J 2019 Concurrency Computation Practise and Experience

[14]] Emam, M. M., Aly, A. A., &Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications, 1(7), pp. 361-366, (2016).

[15] Pandit, A. S., Khope, S. R., & Student, F. Review on Image Steganography. International Journal of Engineering Science, 6115, (2016).