International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

SECURED TEXT TO IMAGE ENCRYPTION USING ASCII VALUE ENCODING

ASWINI A[1], RADHIKA V[2], YAMINI V[3]

[123]*Dept of Software Engineering, VIT University, Vellore, India*

Abstract - *In this paper, we propose a text to image technique to do the hiding of text inside the image. This method involves the storing the value of ASCII in the image's X, Y coordinate. The Ascii value is stored in one of the three Red, Green, or Blue channels, where the other two channels correspond to the message's next coordinate. To generate the random keys, the system involves picking up of the random images of size 256*256.The decryption process involves production of the decrypted text file which has the message. The system is secure and could be combined with the other encryption standard algorithms to make it even more secure.*

Key Words: *Encryption, Decryption, Cryptography, ASCII, Steganography, image, text.*

1. INTRODUCTION

The text to image encryption plays a vital role in the modern era for the information security. In the information security applications, algorithm is used to encrypt data before transmitting it to a remote machine. Hackers are finding a way to steal the confidential data's. So protecting our data's is very much important.

The text to image encryption involves the message that is transmitted in an unreadable format with image to hide the text or the information. The message is sent by converting it to its corresponding ASCII values and are stored in the RGB image of size 256*256.ASCII values of the text ranges from 0 to 128.The encryption process involves the use of the message and the private and public keys to encrypt the text. Decryption is the reverse of the encryption process which involves the method of reverting the encrypted text to its original plain text for the receiver.

2. LITERATURE REVIEW

This paper[1] proposes the image encryption for secured internet multimedia applications. The image is first compressed and then encrypted. The compression is done using discrete wavelets transform. This DWT compress the image into series of frequency bands and then produces two images an average and a detailed image. The average image is discarded and detailed image is used for high resolution.

The compressed image is then encrypted using Data Encryption Standard algorithm.

This paper[2] proposes a technique called selective Encryption for securing the text over wireless Networks. Instead of encrypting the text this selective encryption method encrypts only the important texts. Usually the wireless network devices use battery and it finds difficult for a sensor to spend more computational cost on encrypting and decrypting. Hence by applying the selective Encryption Method over the Ad hoc networks the processing time is reduced which also increases the scalability of data transmission.

This paper[3] proposes a technique of converting a text to image and then applying encryption on it. The text is converted to an image by using RGB substitution where each character of the text is assigned to a pixel randomly and an image is created through it. The image is then encrypted using Advanced Encryption Standard Algorithm and the decryption occurs in reversed way. This proposed method is highly safe because even if the attacker tries to decrypt the output would be an image.

This paper[4] proposes the various chaotic map techniques for image encryption. The 2D chaotic cat Map is generalized to 3D cat map, applying the 3D cat map on the image that needs to be encrypted helps to shuffle the image pixels and positions. Shuffling the pixels is done using two chaotic stages one is Confusion and other is Diffusion. Due to shuffling there occurs lot of confusion and difference between the plain image and cipher image. So that the resistance to attacks and security is increased which makes the image secured.

This paper[5] proposes a method of protecting the text or image from the attacks. They use a method called as persuasive cued click points which represents graphical password technique. This method helps to create a picture password lock to the user by clicking some cued points on the image and then encrypts it using improved AES. Whenever a user needs to secure something he needs to login by selecting any random images from the server then selecting click points and registering it. After login, the user enters the text or image, they are then encrypted using improved AES.

This paper[6] presents the concealing of text within an image by using the approach of the Most significant bit. Image processing techniques are been applied over a selected area of the image. The chaos technique is being used to prevent the breaches. The process is done in an repetitive manner until we get the image fully concealed. CA is applied here to reduce the extent of the image. The evaluation showed that the use of GLCA method and principal part analysis were effective. Error information is calculated to retrieve back the real image.

This paper[7] proposes the disguising of the text in an image using the Fibonacci mode. The content is retrieved from the sender that is to be hidden and compute its size. Produce the Fibonacci series of the text to convert into the matrix. The key is generated from the image. The decrypt of the image is done by subtracting of the enciphered data with the key picture which in turn results in actual text .ASCII code is obtained which in turn is converted to its corresponding letters of the message and by this way the original message is obtained.

This paper[8] proposes the enciphering using the chaotic technique. Distinctive data's are extracted. Add-image-feature procedure is applied here. The key here is the chaotic number which is selected by the sender. Chaotic sequence is generated by the chaotic number and the distinctive data chosen. The series is ordered in any pattern. The algorithm can be able to restore the original data without any loss of data. The performance of the method is calculated and hence t shows it is practical to prevent against the intrusion of attacks.

This paper[9] suggests the hiding of text with the LSB method. The message is first compressed and then encoded. The data is converted to binary. Steganography is used to hide the data. The waterboarding is also used in this paper. The message is divided to set of components. ASCII value was calculated for each of the components. The LSB method is applied on the outlying image and encoded text. Reversal action of the method gives the deciphered text. The LSB along with the other add-ons in this procedure helps to give security to the system.

This paper[10] presents the concealing of data using the Blowfish technique. This paper uses the three phases of providing image concealing. Firstly, the image is encrypted by the use of blowfish and the size of the key is verified for its limit.. Then the data conceal to the enciphered image is done by the LSB method. Any image of interest to sender is chosen which will be the image that binds the enciphered image and the confidential data. The image is then sent to the receiver. The process enhances the security level of embedding different approaches.

3. PROPOSED SYSTEM

3.1. STEGANOGRAPHY

The steganography is a technique of disclosing a file, message, image or video within another file, message image or video. In the project the system involves converting the text into an image and hiding the image with private key and public key images. Usually the steganography doesn't implement the way to remove the image overlays. In the system, we have removed the overlays of the public key and private key images to get the decrypted text.

3.2. TEXT MESSAGE

The user gives the text message which is converted in the form of image by storing the ASCII value in an X, Y co-ordinate of the image. The ASCII value is stored in one of the three Red, Green and Blue channels while other two channels correspond to the next co-ordinate of the image.

3.3. PRIVATE AND PUBLIC KEY IMAGES

The public and private key images are used as mask to cover the text image. The private and public key images are not the same images instead it gets the random image from the website and saves it in the system of the user. Image name is also important to protect the images being rewritten. The image from the internet should be in the size of 256*256 Image with random Red, Green and Blue channel values because it helps to obscure ascii image pixels.

URL used:
https://picsum.photos/256/256/?random

3.4. ENCRYPTION

The encrypted image is created by combining public key image, private key image and the text image. All the three images are first converted into RGB values and they are written to the text file which creates a new encrypted image. The new encrypted image is converted to RGB values and stored as an encrypted image.

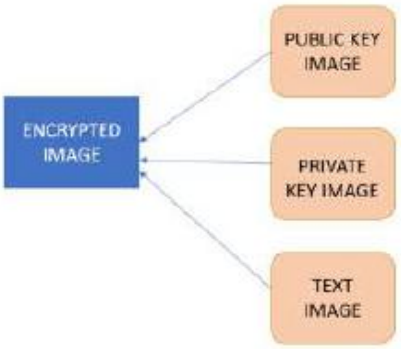


Fig -1: Encryption

3.5. DECRYPTION

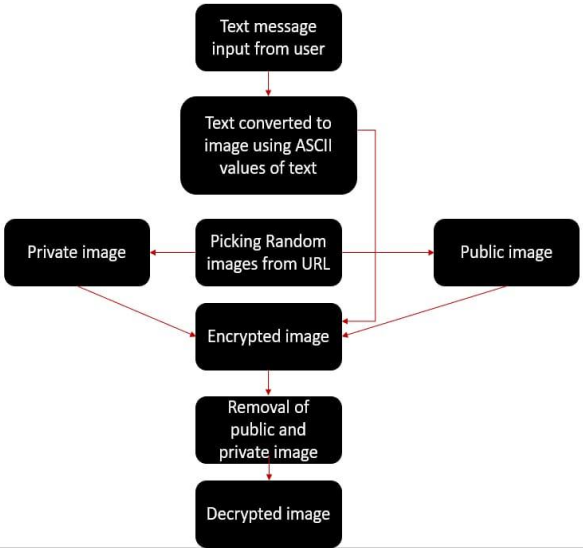
The decryption also imports all the three public, private and text images. The decryption removes all the red, green and blue pixels from every public key image, private key image and text image. After decoding all the RGB values, the decrypted text the original text message is received.

4. WORKFLOW

STEP 1: Get a message from the user and save it in text file.

STEP 2: The ASCII value of the text is stored in the image to create the message image.
STEP 3: The block is replaced with 3 color codes R, G, B for each pixel within the block.
STEP 4: The entire known pixel contain 3 components like Red, Green and Blue. The algorithm has 3 components range between 0 to 255 simultaneously ASCII table also contain 0 to 255.
STEP 5: Load the public key and private key images and combine them with the message image.
STEP 6: The combination of public key image, private key image and message image creates an encrypted image.
STEP 7: Decode the encrypted image using RGB values.

5. ARCHITECTURE



6. RESULT AND DISCUSSION

The system of text to image encryption works on the python platform. The system works on the RGB image. The system is useful for encrypting the text to corresponding ASCII and it is encrypted inside the image and with the help of public and the private keys. The decryption allows for the visual of the plain text.

The message or the information to be sent is placed in a text file and the message is replaced to its respective ASCII values and the message is concealed in an image which is used for further process.

Fig -2: 256*256 image with text hidden

Fig -3: Public Key Image

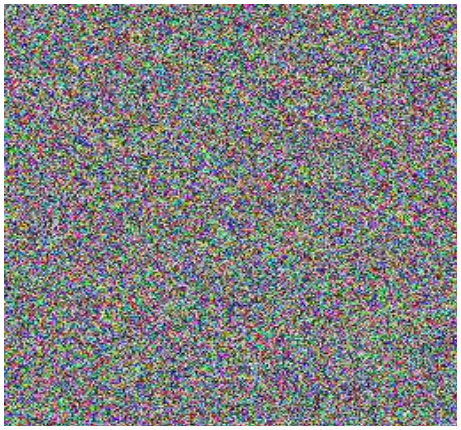


Fig – 4: Private Key Image

The public and the private key images are generated from the link and saved in the sender's system. The image file is also been renamed to avoid the image been rewritten.

Fig -5: Encrypted Image

The encrypted image involves the fashioning of the private key image, public key image and the text. Get RGB values from all three images and write RGB values to txt file. Compute the new encrypted as combination of three image.

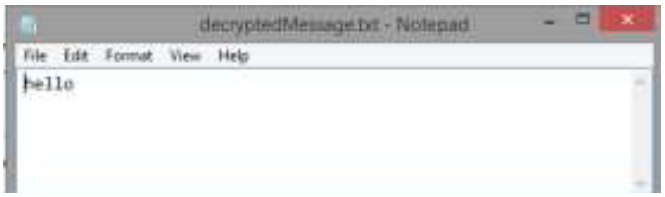


Fig -6: Decrypted text

Decryption algorithm was applied to extract the message that was encrypted.

7. CONCLUSION

This paper discusses how the data or the information could be securely sent from sender to the receiver via the usage of the image as the object to hide the message. The proposed method is secure and the receiver could get the text sent by the sender safely .With this implementation, one problem we have is the safe transfer of the private image to the other person. It needs to be done through a secure channel like physical media at the moment. It would be ideal in a future analysis to introduce some mathematical operations to send and deliver this data. The proposed method is very useful for securely transmitting the message between sender and receiver.

8. REFERENCES

[1] Dang, P. P., & Chau, P. M. (2000). Image encryption for Dang, P. P., & Chau, P. M. (2000). Image encryption for secure internet multimedia applications. IEEE Transactions on consumer electronics, 46(3), 395-403.

[2] Kushwaha, A., Sharma, H. R., & Ambhaikar, A. (2016). A novel selective encryption method for securing text over mobile ad hoc network. Procedia Computer Science, 79, 16-23.

[3] Joshy, A., Baby, K. A., Padma, S., & Fasila, K. A. (2017, November). Text to image encryption technique using RGB substitution and AES. In 2017 International Conference on Inventive Computing and Informatics (ICICI) (pp. 1133-1136). IEEE.

[4] Gagnani, L. P., & Varjani, S. (2015). Survey of 3D Chaotic Map Techniques for Image Encryption. International Journal of Science and Research (IJSR) ISSN (Online), 2319, 7064.

[5] Chaturvedi, S., & Sharma, R. (2015). Securing Text & Image Password Using the Combinations of Persuasive Cued Click Points with Improved Advanced Encryption Standard. Procedia Computer Science.

[6] Talwar, D., Bansal, D., & kaur, M. (2019). Secure Text Hiding Method in Image Processing using Enhanced MSB Technique . International Journal of Soft Computing and Engineering, 9(3).

[7] Mukherjee, M., & Samanta, D. (2014). Fibonacci Based Text Hiding Using Image Cryptography. Acharya Institute of Technology, Department of MCA, Bangalore, India, 2(2).

[8] Deng, Z., & Zhong, S. (2019). A digital image encryption algorithm based on chaotic mapping. Journal of Algorithms & Computational Technology, 13, 1748302619853470.

[9] Tavoli, R., Bakhshi, M., & Salehian, F. (2016). A New Method for Text Hiding in the Image by Using LSB. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 7(4), 126-132.

[10] Agarwal, D., panwar, P., & vyas, P. (2019). Enhancing Image Security by employing Blowfish Algorithm further embedding text and Stitching the RGB components of a Host Image. International Journal of Recent Technology and Engineering, 8(2S11).