ANDROID BASED APPLICATION FOR FILE ENCRYPTION/DECRYPTION

Nitesh Ramakrishnan[1], Chappa Sai Chaitanya[2], Sudhaghar J[3], Muthamil Selvan S[4]

[1] Student, Department of Computer Science, SRM Institute of Science and Technology, Tamil Nadu, India.
[2]Student, Department of Computer Science, SRM Institute of Science and Technology, Tamil Nadu, India.
[3]Student, Department of Computer Science, SRM Institute of Science and Technology, Tamil Nadu, India.
[4]Assistant Professor, Department of Computer Science, SRM Institute of Science and Technology, Tamil Nadu, India.

ABSTRACT

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot view the contents. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can be read only if decrypted. Our Proposed System is an android based application that enhances the encryption technique to the next level by encrypting / decrypting the given data using the mobile phone itself. The encryption technique will compress the given text into an image or a file which cannot be viewed by an unauthorized user easily because the encrypting algorithm is different every time. The pixels of the selected image is broken down into tiny bits and the given code is combined with these bits which together will form the encrypted image. Here the data stored is hidden inside the image, while seeing from outside it is viewed as a simple image but only upon applying the encryption key the data and the image will be decrypted and thus it is very secure. There are many software's which can encrypt or decrypt a file but it will take more process time and memory to complete but using the application the encryption can be done easily and the data can be shared easily.

Keyword: - *Encryption, Decryption, Android, Cipher text.*

1. INTRODUCTION

Encryption is a process which uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data. With the help of key and the algorithm we can encrypt or Decrypt the plaintext into cipher text and then cipher text back into plaintext. Image encryption plays an important role in the field of information hiding. Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet.

2. EXISTING SYSTEM

An Encryption software is used to convert the data into cipher text, this software will use various algorithms, techniques so that the encrypted data is very secure and confidential. This software is done using high specifications computer. This method is similar as steganography where the text will be represented by an image. In the traditional architecture there existed only the server and the client. In most cases the server was only a data base server that can only offer data. This makes maintenance expensive.

3. PROPOSED SYSTEM

This android based application that enhances the encryption technique to the next level by encrypting/decrypting the given data using the mobile phone itself. The encryption technique will compress the given text into an image which cannot be viewed by an unauthorized user easily because the encrypting algorithm is different every time. The pixels of the selected image is broken down into tiny bits and the given code is combined with these bits which together will form the encrypted image. Here the data stored is hidden inside the image, while seeing from outside it is viewed as a simple image but only upon applying the encryption key the data and the image will be decrypted and thus it is very secure. We use the AES, RSA algorithm to encrypt or decrypt the file. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm.

It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. The android application lets the user to convert a set of information into an encrypted image which cannot be read easily. Using the key only it can be decrypted, thus it is very secure.

4. WORKING

The android based application will work on any smart phone which is connected to the internet. it will be a simple user interface such that anyone can use it with ease. The application runs on different phases to complete the process.

4.1 USER INTERFACE

The user has to input the plain text in the given space and select the file or image to which it needs to be encrypted. After selecting the file the user has to press the encryption button.

4.2 ALGORITHM

```
1. Received blocks of nXn image along with encrypted key.
2. 128-bit AES ->Dn (blocks, 1..b)
3. Extract(En(information))
4. 128-bit AES ->Dn (Information);
        4.1 First block ->Dn (label + LSB of block+ r1+ b)
        4.2 Last block ->Dn (Label+ LSB of block +rb+ one bit extra to show end of the blocks).
        4.3 Intermediate blocks ->Dn (Label+ LSB of block +[r2 ... rb-1])
5. Collect LSBs of all the blocks and combine to form a sequence of bits.
If blocks LSB (block 1)+ LSB(block2)+ … LSB(block b) == K LSB (block 1)+ LSB(block 2)+…LSB(block b)
Then “Image not corrupted”
Else “Image corrupted”
6. Based on the step 5 combine the blocks to form a complete original image.
```

4.3 ENCRYPTION/DECRYPTION

In this phase the user has to select the option of encrypt or decrypt so that accordingly the input is taken for processing. The image will be split into blocks or pixels which combines with the given input text and algorithm takes care of this. For decryption the user has to select any encrypted file which has hidden contents. Then algorithm authenticates the key and decrypts the information in the file.

4.4 OUTPUT:

The encrypted file or image is directly stored in the specified storage location. The user can change the location anytime in the settings. The user has to navigate to the required folder to retrieve the encrypted file for further sharing and decryption process. The output file can be shared easily using any messenger or mail etc.

5. MERITS

- Minor errors can be rectified.
- Image sizes can be increased or decreased.
- Reduces manual work
- Unrecognizable features can be made prominent.
- Very secure
- More accurate and efficient

7. ARCHITECTURE DIAGRAM

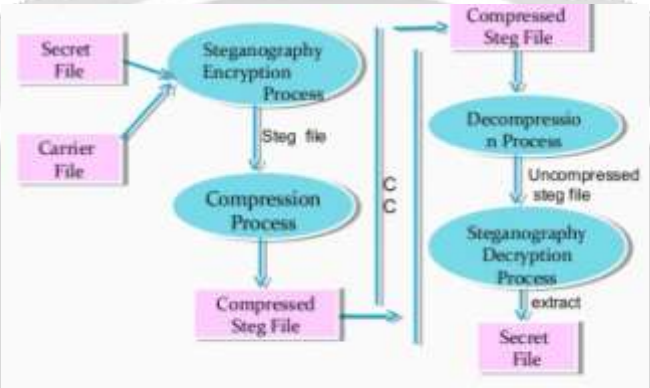

Fig -1: System Architecture

8. CONCLUSION

The mobile application, incorporating the application based encryption technique, is a very effective tool which can be used for improving the overall security of an information. The proposed mobile application portability and ease in use increases its credibility compared to other state of - art methods.

9. FUTURE WORK

This application can be future enhanced by adding some more security features like fingerprint scanner as key. This will make the app even more secure. The next step in this direction will be system implementation, calculating time and space complexity for the same using some experimental data and then comparing it with existing algorithms and schemes for its efficiency, accuracy and reliability. If this application is implemented the data security percentage will increase by a huge margin.

10. REFERENCES:

[1]. Pareek K. Narendra, “design and analysis of a novel digital image encryption scheme” International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[2]. Naskar Kr. Prabir, Chaudhuri Ayan, Basu Debarati, Chaudhuri Atal “A Novel Image Secret Sharing Scheme”, Second International Conference on Emerging Applications of Information Technology, IEEE xplore, 2011

[3]. Lee Jung-San , Le T. Hoang Ngan, “Hybrid (2, n) Visual Secret Sharing Scheme for Color Images”. IEEE xplore, 2009

[4]. Asim Muhammad, Jeoti Varun, “Hybrid Chaotic Image Encryption Scheme based on S-box and Ciphertext Feedback”, International Conference on Intelligent and Advanced Systems, IEEE xplore, 2007.