INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 4)
Available online at: www.ijariit.com

Securing image document using RSA

Omkar Prakash Dalvi
omkarpd95@gmail.com
Veermata Jijabai Technological Institute, Mumbai, Maharashtra

ABSTRACT

It is difficult to store and secure all information or data in paper format which also creates a problem for a proper search, storing and durability of information. Increase in new smart technologies and ease of living has developed various ways to share small and vital information digitally with the use of various applications and devices. But as the ways of sharing information and technologies are increasing, the risk of misusing the information is also increasing. Protection and security of information is a necessary feature of such applications, software or devices which handle such information. In the case of images, the security systems still lack to provide security. As the increase in digitization, the documents such as identity proof, educational qualification, and various certificates are uploaded online on various government or private website and mobile applications to verify proper identification or eligibility of documents related to that person. Such uploads of documents or proofs are done in image format. But sharing of this information may lead to a serious loss or misuse of that information. This paper deals with securing image with the use of OCR and RSA algorithm for securing the information The image would be converted into text file and the generated text file would be encrypted and send through the network to the destination and again reverse or decryption process will be followed on the other side and text file will be again generated to its image form.

Keywords— *Optical Character Recognition (OCR), Rivest-Shamir-Adleman (RSA), Security*

1. INTRODUCTION

Security and time are two essential features to create an essential system. Instead of overlapping an image for providing its security, this could increase the risk of attack. And if the image document consists of important information of a particular person or organization it may cause a great loss to that person or that organization. It could also lead to forgery of a document. The document may consist of contracts, license, identification cards and certificates, etc. Such documents can face file upload vulnerability attack, through which the attacker can detect the image uploaded by the user and could misuse or modify the image or modify the information contained in that image. Such attacks are commonly done in web-based applications. Encrypting an image could increase the security and such attacks can be avoided. But encrypting the image with the help of pixel replacement or pattern are less effective to overcome this problem the algorithm should be properly processed.

The encryption should be in such a way that the person to whom the document is sent for verification or any other purpose should only know about the data or access the information. In this paper, the image document is secured by converting the image into a text file and applying RSA algorithm on that text document and sending this encrypted file to the network or to the destination and again decrypting it back into image form.

2. RELATED WORK

Majority of web-based application does not provide proper security when it comes to uploading of an image. The basic encryption used for encrypting an image is replacing the pixels or bits of an image and sending it to its destination over a network but it does not provide a full-fledged security since the size of the image remains same and the detection and replacement could be done by the attacker to regain the original form of the image on the bases of size and patterns that could form.

To overcome this problem a key-based algorithm can be used. The key-based algorithm could be a symmetric or asymmetric key algorithm. And the strength of the encryption in key-based algorithm depends upon the size of the key used during the encryption process. The symmetric key algorithm is the algorithm in which the same key is used in encryption and decryption. The asymmetric algorithm is the algorithm in which two different keys, the public key and private key are used for encryption and decryption process.

OCR stands for optical character recognition it detects the character from the image file and helps to convert the image file into a text file or text document.

RSA is an asymmetric key algorithm. An asymmetric key means it has two keys public key and private key for encryption and decryption. The public key is a key which can be shared to everyone and the private key is the key which is kept secret or private. Since it is difficult to factorize a large integer RSA also works on the same idea. It works by taking up two large prime numbers p and q. Calculating n=p*q and phi=(p-1)(q--1), Now taking e which will be the public key such that e should be coprime of phi(n) and gcd(e, phi(n))=1. And this e will be used up in encryption of the data. Now calculation of the private key or also called as the secrete key which is denoted by d. Now d will be in such a way that $d \equiv e^{-1} \bmod phi(n)$, which can also be calculated as $ed \equiv 1 \pmod{phi(n)}$ i.e. d*e mod phi(n)=1. Now the public key={e, n} and private key ={d, n}. The plain text should be less than n and the encryption process or cipher text denoted by c will be c= plain text ^{e} mod n and the decryption process i.e. converting cipher text to plain text will be as plain text $=c^{d}$ mod n.

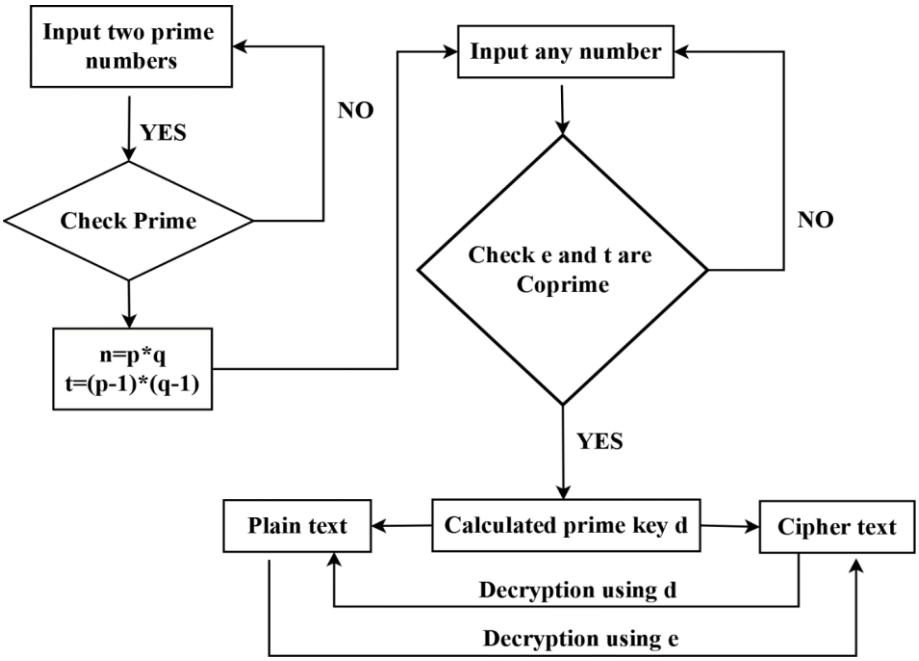

Fig. 1: Working of RSA

3. PROPOSED WORK

3.1 Secure sharing of image document using OCR and RSA

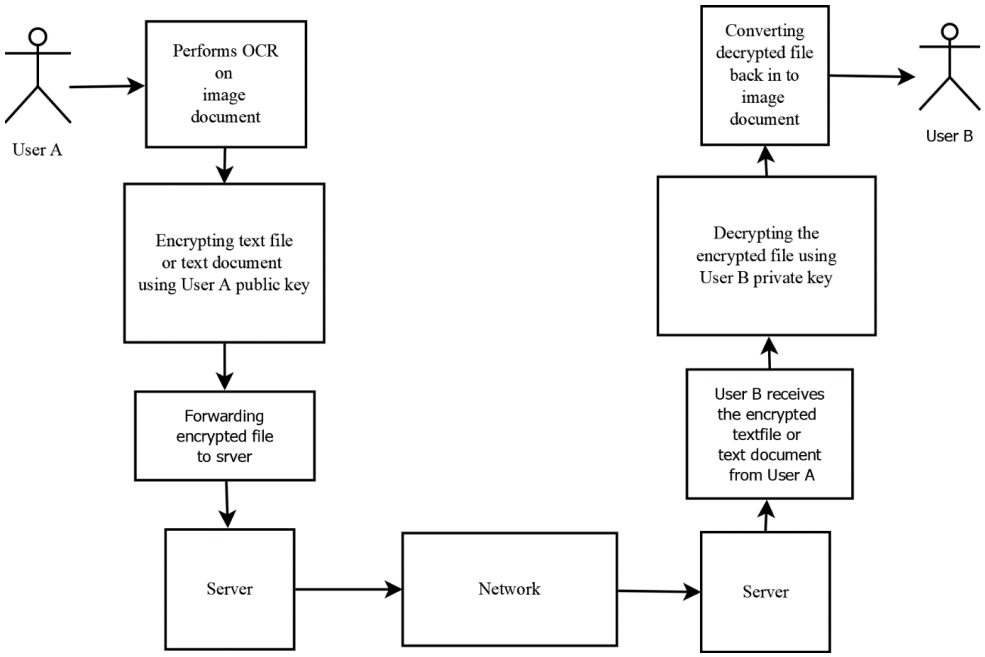

Fig. 2: Secure sharing of image document using OCR and RSA

(a) User A selects the image document that is to be uploaded or send to User B
(b) OCR is performed on the image document and converted into a text file or text document for encryption
(c) The encryption process is done using the RSA algorithm. The file is encrypted using the public key of User A
(d) The encrypted file is forwarded to server and from server to network
(e) User B receives the encrypted file from the server
(f) Decryption process takes place using the RSA algorithm. The encrypted file is decrypted using the private key of User B
(g) Now, the decrypted text file is converted to an image

4. IMPLEMENTATION AND RESULT

In this section, we will discuss the implementation of securing an image document using OCR and RSA. Figure 3 is the login screen of the system. For a better authentication of the users for the process, a login is created.it contains username password and IP address of the system through which the user will log in. In Figure 4 we can see the OCR screen. User can log in to the screen and select the image document through the system which to is sent or need to upload. Optical Character Recognition process is used to detect and convert the information into a text file present in the image file.

In figure 5 the text file or text document that is converted is then encrypted using the RSA algorithm. The encryption is performed using the public key of the user. For example, User A needs to send image X to User B, The User A will convert the image into text and encrypt the text document using the public key of User A and it would be sent to server and then in to network to User B. User B will receive the encrypted text document and it will decrypt the text document using private key of the User B. and will convert the text file back into image file.

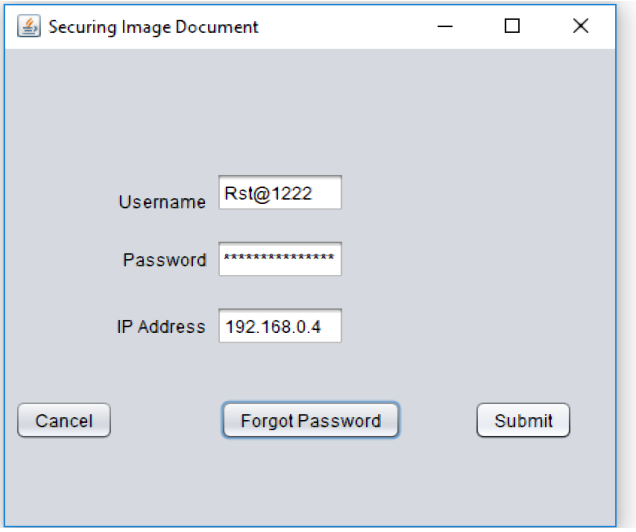

Fig. 3: Login screen

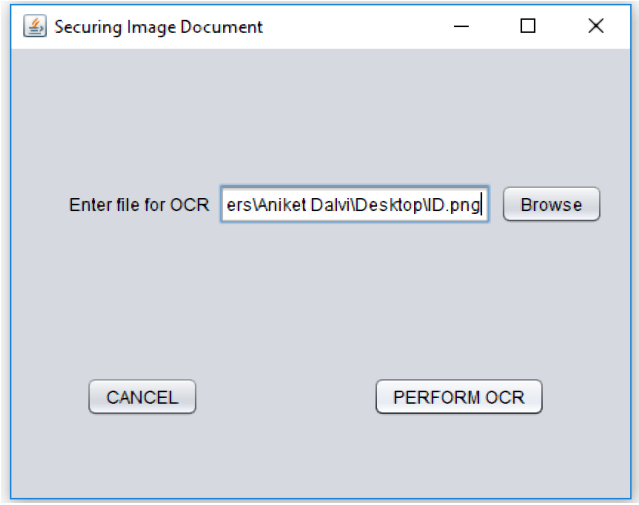

Fig. 4: Performing OCR on image document

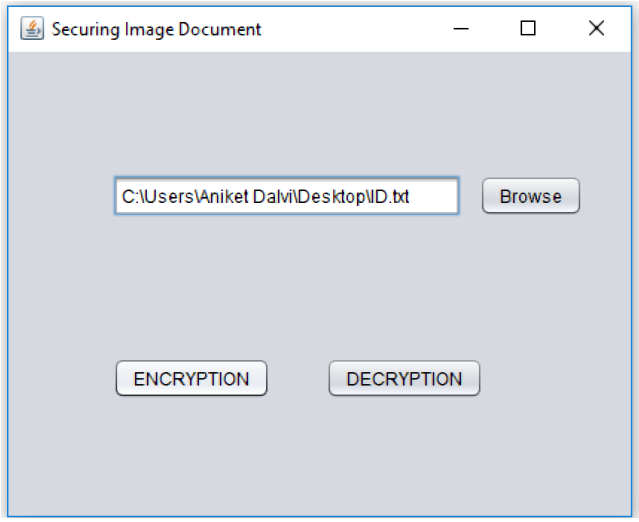

Fig. 5: Applying RSA on the text document

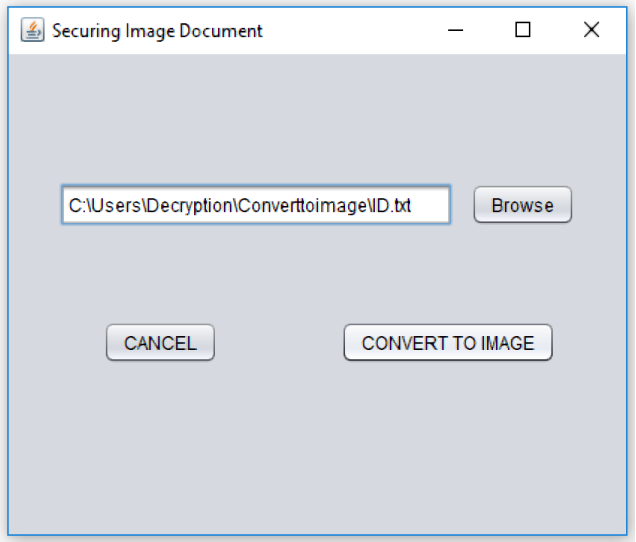

Fig. 6: Converting to image format after decryption

For example, User A needs to send image X to User B, The User A will convert the image into text and encrypt the text document using the public key of User A and it would be sent to server and then in to network to User B. User B will receive the encrypted text document and it will decrypt the text document using private key of the User B. and will convert the text file back into image file.

5. CONCLUSION AND FUTURE SCOPE

Converting the image file into a text file and encrypting the text file and decryption on the receiver's side decrease the risk of attack through detection of pattern and it can also decrease file vulnerability attack. By using an asymmetric key algorithm for encryption and decryption there is no chance of sharing a key on a network. Since encryption is done through the public key and decryption is done through the private key of the receiver. It also solves the problem of picture or text visibility in an image. Since with the help of OCR, it could also detect the information in the low-quality images and can convert it into a text document.

As the actual size and encrypted size of the image differs the possibility of detecting an image through formation or pattern also gets secure due to the use of keys in encryption and decryption. The proposed work can be extended through the use of Elliptical Curve Cryptography for encryption and decryption. Since it uses the lower key sizes than RSA.

6. REFERENCES

[1] B. Persis Urbana Ivy, Purshotam Mandva and Mukesh Kumar -A modified RSA cryptosystem based on n prime International Journal of Engineering and Computer Science.
[2] Dan Boneh and Victor Shoup Applied Cryptography
[3] Anil Kumar and Rohini Sharma A secure image steganography based on RSA algorithm and Hash-LBS Technique International Journal of Advance Research in Computer Science and Software engineering
[4] Li donjiang, wng Yandan, Chen Yong Research on Key Generation in RSA Public-key Cryptosystem IEEE
[5] M. Revow, C. K. I. Willams , G. E. Hington Using generative models for hand written digit recognition IEEE
[6] NaQi, Wei Wei, Jing Zang, Wei Wang, Jinwel Zaho, Junhuai li, Pery Shen, Xiyoyan Yin , Xingarong Xiao and Jie Hu Analysis and research of RSA algorithm Information technology Journal.
[7] Muhammad Ghiya , R. Marwati, S. Gozali Hybrid algorithm of RSA and one-time pad Cryptography Academia
[8] Vikas Tyagi Image Steganography using a least significant bit with cryptography international journal of Global research in Computer Science
[9] Ajit Singh, Swati Malik Securing Data by Using Cryptography with Steganography International Journal of Advance Research on computer science and Software Engineering.
[10] Rajendra Kaur, Er. kawalprit Singh Image Encryption Techniques a Selected Review IOSR Journal of Computer Engineering

