



Image Cryptography Using RSA Algorithm in Network Security

S.Anandakumar

*Research Scholar, School of Computer Science, Engineering and Applications,
Bharathidasan University, Tiruchirappalli*

Abstract- In today's era it is a crucial concern that proper encryption decryption should be applied to transmit the data from one place to another place across the internet in order to prevent unauthorized access. Image Cryptography is a special kind of encryption techniques to hide data in an image for encryption and decryption of original message based on some key value. Very few algorithms, provides computational hardness and it makes difficult to break a key to find the original message. Here RSA algorithm is used to encrypt the image files to enhance the security in the communication area for data transmission. An image file is selected to perform encryption and decryption using key generation technique to transfer the data from one destination to another.

Keywords- RSA Algorithm, Images, Symmetric Key, Asymmetric Key, Key Generation, Prime Numbers, Hex Code

I. INTRODUCTION

Internet is the medium in the increasing growth of multimedia to transfer from the data from one place to another place across the internet. There are many possible ways to transmit the data over the internet such as e-mails, sending text and images, etc. In the present communication images are widely use. One of the major issue with transfer the data over the Internet is the security and authenticity. The security is basically protecting the data from an unauthorized users or attackers. Encryption is one of the technique which is use for secure the information. Image encryption is a technique that convert original image to another format with the encryption techniques. The same way in the decryption no one can access the information without knowing a decryption key.

Image security is an utmost concern in the web attacks are become more serious. The Image encryption and decryption has applications in internet communication, military communication, medical imaging, multimedia systems, telemedicine, etc. To make the data secure from various attacks the data must be encrypted before it is transmit. The government, financial institution, military, hospitals are deals with confidential images about their patient, financial status, geographical areas, enemy positions. Most of this information is now collected and stored on electronic computers and transmitted over the network. If these all the confidential images about enemy positions, patient and geographical areas are get in the wrong hands

such a security could lead to declination of war, wrong treatment etc. Protecting the confidential images is the legal requirement. So has to make a strong encryption for a image so that it can't be hacked easily. And the perfection in the original image can obtain after decrypting it.

An another use of internet could be transfer the secure data which may be very essential for a group of companies, that the data should not be view by others. Therefore sensitive data hiding becomes most important area in securing network information. The method is use for secure the data is known as encryption. After encrypting the data, with the help of network it is transfer to the destination. At its destination encrypted data is decoded with the help of provided algorithm which is known as decryption. The private or sensitive information will be hidden within an image, and it is transmit with the secure keys which then decrypted.

RSA is an algorithm which is use provide the encryption and authentication system. This is developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. This algorithm is most commonly used encryption and authentication algorithm. The RSA algorithm is one of the first public key cryptosystems, and it is widely used for secure the data transmission. In such a cryptosystem, the encryption key is a public one and the decryption key is differ which is keep secret. In RSA, this asymmetry is based on the product of two large prime numbers, the factoring problem. The RSA encrypt key is encrypt the image, so that it convert into cipher text format and it will be store as a text file. The opposite method of encryption, the reverse process is compute by another one decryption key of RSA algorithm and it decrypts the image from the cipher text. Finally it will discover the resultant image by the decryption techniques.

II. PURPOSE OF CRYPTOGRAPHY

Cryptography provides security to ensure the privacy of data, non-alteration of data and so on. Nowadays cryptography is widely using due to the great security. There are the various cryptography goals are following as,

A. Confidentiality

The transmission of data from one computer to another computer has to be accessed by an authorized user and it not access by anyone else.

B. Authentication

The transmission of data from one computer to another computer has to be accessed by an authorized user and it not access by anyone else.

C. Integrity

Only the authorized party is allow to modify the transmitted information. And an unauthorized persons should not allow to modify in between the sender and receiver.

D. Non Repudiation

Ensures the message that sender or the receiver should be able to deny the transmission.

E. Access Control

The authorized persons only able to access the information while in transfer.

III. TYPES OF CRYPTOGRAPHY

Cryptography technique is secure the secret message when it is transfer from one place to another place over the networks. The cryptography contains the two main categories which are following as,

- 1) Symmetric key cryptography
- 2) Asymmetric key cryptography

A. Symmetric key cryptography

Secret key cryptography is also known as symmetric key cryptography. In this type both the sender and the receiver know the same secret key. The sender is encrypt the data or the information using the secret key and the receiver is decrypt the information using the same secret key. In the symmetric cryptography the key is playing a very important role which is depends on the nature of key.

B. Asymmetric key cryptography

Asymmetric cryptography is used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys. Public key cryptography, also called asymmetric key cryptography which is using a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The cryptography technique is using the secret message transfer from one place to another place over the networks. The cryptography technique is require some algorithms for encrypt the data.

IV. RELATED REVIEW WORKS

Gunasekaran G. and Bimal Kumar Ray, et.al. [7] proceeded the technique which is used for securing data is known as encryption. The encrypted data is transfer through the network. And the encrypted data is decrypt using provided algorithm which is known as decryption. The secret information is hide within an image and it is transfer with the secret key. In past times for secure the information using by wax tablets and invisible ink, but now it is a modern society so the security is totally changed. Now a day's images, pictures, videos and voices are carrying the message in transferring from one place to another place with the help of network communication.

Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, et. al. [6] explained about an image cryptography it may use the traditional cryptosystems to encrypt images. But it having two problems. The first problem is that the image size is always much greater than text. So the cryptosystems is need much time to encrypt the image. The second problem is the decrypted data should be equal to the original data. Due to the Characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

Ambika Oad, Himanshu Yadav, Anurag Jain, et. al. [3] recommended the image encryption is a technique which is convert the original image into another format that is difficult to understand. So, without knowing the decryption key no one can access the information. The image encryption has applications in corporate world, health care, military operations, and multimedia systems. Encryption is the process which is encoding the plain text into cipher text, and the reverse process of converting cipher text into the plain text is decryption. The cryptography consists of encryption and decryption techniques.

Komal D Patel, Sonal Belani, et. al [2] suggested the image encryption techniques are convert the original image to another image that is hard to understand, it is keep the image confidential between users. It is essential that nobody can't to get the information without a key for decryption. Furthermore, special and reliable security in transmission the digital images is needed in many applications, such as military image communications, cable-TV, online personal photograph album, medical imaging systems and confidential video conferences, etc. In order to fulfill such a task, and have been proposed many image encryption methods.

V. FUNCTIONALITY OF IMAGE CRYPTOGRAPHY

The image cryptography is work as the flow chart which is shown in the Fig.1. The Fig.1 is describe the step by step manner of processing in the encryption and decryption.

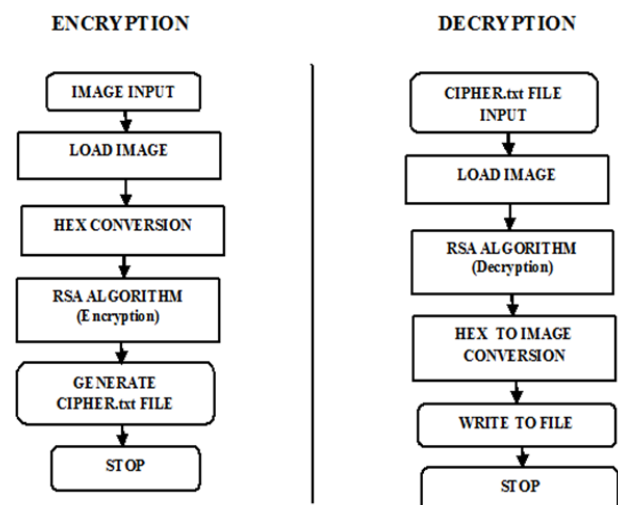


Fig. 1 Encryption and Decryption flow

VI. IMAGE CRYPTOGRAPHY METHODOLOGY BY RSA

The RSA is an cryptographic algorithm which is use to encrypt and decrypt the data. This algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA cryptosystem is also known as the public-key cryptosystems. RSA is normally used for secure data transmission.

The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret. The public key is used to encrypt a message, and private key is used to decrypt a message or information.

The RSA algorithm is encrypt the original image and decrypts the image by the different keys. That is shown in Fig.2.

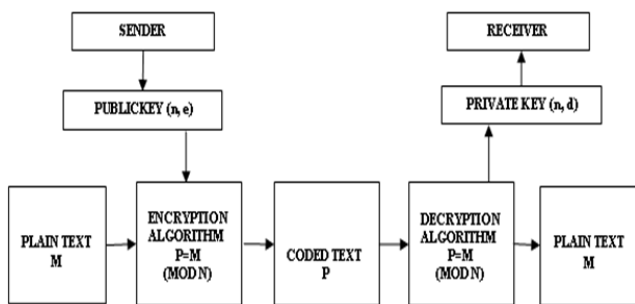


Fig. 2 RSA Diagram

VII. RSA ALGORITHM

RSA is an algorithm is using in the modern computer environment to encrypt and decrypt the data in transform. The RSA algorithm is also called as an asymmetric cryptographic algorithm. Asymmetric cryptosystem means two different keys are using in the encryption and decryption. In the two keys one key is using for encryption and the second key is using for decryption. This RSA algorithm is also called as the public key cryptography. Because one of the secret key can be given to everyone which means public. The other key must be kept private.

The RSA algorithm consists of three manor steps in encryption and decryption. The steps are following as,

- 1) Key Generation
- 2) Encryption
- 3) Decryption

A. Key generation

The key generation is the first step of RSA algorithm. The RSA involves a public key and a private key. On those keys the public key can be know everyone and it is use for encrypting messages. Messages encrypted with the public key can decrypt using the private key. The keys for the RSA algorithm is generated by the following steps,

- 1) First choose the two distinct prime numbers p and q .
- 2) For security purposes, the integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primality testing.

- 3) Then compute the n value, $n = pq$.
- 4) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- 5) Compute $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where ϕ is Euler's totient function. This value is kept private.
- 6) Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; i.e., e and $\phi(n)$ are co-prime.
 e is the released as the public key.
 e has a short bit-length and small Hamming weight results in more efficient encryption.
However, much smaller values of e have been shown to be less secure in some settings.
- 7) Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\phi(n)$). This is stated as, solve the d given $d \cdot e \equiv 1 \pmod{\phi(n)}$. This is computed using extended Euclidean algorithm. It using the pseudo code in the Modular integers section, inputs a and n correspond to e and $\phi(n)$, respectively.
- 8) d value is keep as the private key.

The public key consists of the modulus n and the public key e . The private key have the modulus n and the private key d , and it keep in secret. p , q , and $\phi(n)$ values are keep in secret, because they can be used to calculate d .

B. Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key d secret. Bob then it is wish to send the message M to Alice.

So, first turns M into an integer m , such that $0 \leq m < n$ and $\gcd(m, n) = 1$. Then it compute the cipher text c .

This can done efficiently, even the numbers are 500-bit numbers, it is using the Modular exponentiation. Bob then transmits c to Alice. At least nine values of m will yield a cipher text c equal to m .

C. Decryption

Alice can recover m from c by using her private key exponent d via computing. Given m , she can recover the original message M by reversing the padding scheme.

VIII. APPLICATIONS OF IMAGE CRYPTOGRAPHY

Core banking is a set of services providing by the group of networked bank branches. Bank customers may access their funds and perform the simple transactions from the member branch offices. The major issue in core banking is the authenticity of the customer. An unavoidable hacking of the databases on the Internet, it is always quite difficult to trust the information in Internet. To solve this problem of authentication proposing an algorithm based on image processing and image cryptography.

The internet multimedia applications is become popular. The valuable multimedia content such as the image

is vulnerable to unauthorized access while in storage and during transmission over a network.

The image processing applications have been commonly found in the Military communication, Forensics, Robotics, Intelligent systems etc.

IX. MERITS AND DEMERITS OF IMAGE CRYPTOGRAPHY

A. Merits

One advantage to encryption is that it separates the security of data from the security of the device where the data is transmitted over the Internet. And the advantages to implementing encryption include the pain that comes with data breach disclosures, the provision of strong protection for intellectual property. The people should keep in mind the standard email is not secure and is in fact tantamount to writing sensitive information on postcards. The encrypted data that can only be read by a system or user who has the key to unencrypted the data means the system or user is authorized to read the data. Encrypted data cannot be accessed by the third parties. The encryption is come with the numerous advantages that need to protect the data.

And some another benefit is there in using Image Cryptography. There are,

- 1) Peace of Mind
- 2) Identity Theft Protection
- 3) Safe Decommissioning of Computer
- 4) Unauthorized Access Protection
- 5) Compliance with Data Protection Acts

B. Demerits

The encryption is a very complex technology. One big disadvantage of encryption is related with keys are that the security of data becomes the security of the encryption key. The data is lost effectively if lost that the keys. Encrypting data and creating the keys necessary to encrypt and decrypt the data is computationally expensive. The systems performing is heavy take the available resources in computational. One of the common drawbacks of traditional full-disk encryption solutions are reduction of overall performance of the system deployment key pitfall is that a poor encryption implementation could result in the false of security when in fact it wide open to attack.

X. RESULT AND DISCUSSION

For this, an experimental with the different raw images with the different sizes are encrypted and decrypted. In this paper the cryptography mechanism is using the RSA algorithm with the public key encryption is to increase the security levels of the encrypted. Here one key is needed to encrypt and another key is needed to decrypts the image. Finally the image cryptography experiment is provide the feasibility of security to the image in network security. The data is not view by no one without the knowledge of cryptography.

The image is consist of secret and it is going to be encrypted it is called as an original image may contain the data and it is shown in Fig.3.



Fig. 3 Original Image

The Original image is encrypted by the key which is generated by the RSA algorithm. It is converting the image into the cipher text. It is shown in Fig.4.



Fig. 4 Encrypted Cipher Text

Finally the cipher text is decrypted by another one decrypt key which also generated by the RSA algorithm. And it is convert the cipher text into the resultant image. It is shown in Fig.5.



Fig. 5 Decrypted Image

XI. RESULT AND DISCUSSION

In the digital world, the security of images has become more important as the communication has increased rapidly. All the techniques are in a real-time image encryption could only find a low level of security. Here, the image encryption algorithm proposed efficient and highly securable with high level of security and less computation. The results of the simulation show that the algorithm has advantages based on their techniques which are applied on images. Hence it is conclude that the techniques are good for image encryption and give security in the open network.

REFERENCES

- [1] Payal Sharma, Manju Godara, Ramanpreet Singh, *Digital Image Encryption Techniques: A Review*, International Journal of Computing & Business Research ISSN (Online): 2229-6166.
- [2] Komal D Patel , Sonal Belani, *Image Encryption Using Different Techniques: A Review International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, Volume 1, Issue 1, November 2011.
- [3] Ambika Oad, Himanshu Yadav, Anurag Jain, *A Review: Image Encryption Techniques and its Terminologies*, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.
- [4] Rivest R, Shamir A, Adleman L, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of ACM 21 (2): 120–126. doi:10.1145/359340.359342 (February 1978).
- [5] Calderbank, Michael, *The RSA Cryptosystem: History, Algorithm, Primes*, (2007-08-20).
- [6] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, *Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)*, ISSN 2249-6343 International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.
- [7] Gunasekaran G. and Bimal Kumar Ray, *Encrypting And Decrypting Image Using Computer Visualization Techniques*, Journal of Engineering and Applied Sciences VOL. 9, NO. 5, ISSN 1819-6608, MAY 2014.