INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 08, August 2024, pp: 507-512

Impact Factor: 5.725

ENCRYPTION AND DECRYPTION IMAGES USING RSA ALGORITHM

Rasha Rokan Ismail[1]

[1]Diyala university, Diyala, Diyala, Iraq.

DOI: https://www.doi.org/10.58257/IJPREMS35741

ABSTRACT

In today's world, secure data transmission over the internet takes priority over other activities. Different algorithms exist to provide computational difficulty that makes it difficult to crack the key to identify a unique message. Many researchers have implemented different encryption algorithms to securely transmit data, and different hybrid encryption algorithms have been proposed to improve the level of information security. Key management plays an important role in implementing encryption algorithms. For this reason, we implemented an image encryption technique that uses a random image as a key. I used a random image as a key and encrypted another image as information using the RSA algorithm. The proposed method was compared with conventional methods and it was concluded that encryption algorithms implemented using images as keys provide more security in terms of encryption and decryption times.

Keywords: Encryption , Decryption, RSA Algorithms, Cryptography,

1. INTRODUCTION

Information security has become a central issue in information storage and transmission, it often requires that data be kept safe from unauthorized access. The best line of defense is physical security [1]. However, physical security is not always an option, due to cost and or efficiency considerations. Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use. Cryptography, defined as the science and study of secret writing concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. 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 transmitting. 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 with regard to confidentiality [2].cryptography is used to encrypt data residing on storage devices or travelling through communication channels to ensure that any illegal access is not successful. Also, cryptography is used to secure the process of authenticating different parties attempting any function on the system. Since a party wishing be granted a certain functionality on the system must present something that proves that they indeed who they say they are. That something is sometimes known as credentials and additional measures must be taken to ensure that these credentials are only used by their rightful owner. The most classic and obvious credential are passwords. Passwords are encrypted to protect against illegal usage. Security of internet banking account passwords, email accounts password etc. requires text protection in digital media [3].Unlike text messages, the multimedia information including image data has some special characteristics like

redundancy and high correlation among pixels. One of the main goals that must be achieved during the transmission of information over the network is security. This technique will make the information to be transmitted into an unintelligible form by encryption so that only authorized persons can correctly recover the information. Encryption is the process of transforming a piece of information, known as the plaintext, using an algorithm, known as the cipher, to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment).[4]

2. CRYPTOGRAPHY

The study of mathematical techniques related to aspects of information security such as entity authentication, data integrity, confidentiality, and data origin authentication is called cryptography. It deals with techniques of transmitting information in a secret manner to protect the information from unauthorized parties, even if the transmission is done through an insecure channel. The basic types of cryptographic systems are: symmetric key (or secret key) algorithm, asymmetric key (or public key) algorithm and hash function [5].

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 08, August 2024, pp: 507-512

Impact Factor: 5.725

2.1 Types of Cryptography Model

There are two basic schemes utilized to speed up the cryptographic transformations. The main scheme is to design faster (symmetric or asymmetric) cryptographic algorithms.

2.1.1 Asymmetric Cipher (Public key) Model

It is also known as public-key encryption. One of the cryptosystem forms is asymmetric encryption in which different keys are used in encryption and decryption processes. One of the keys is private and the other is public. One of the keys is used for transforming plaintext into cipher text along with encryption algorithm, while the other key is used to restore the plaintext from the cipher text with the help of decryption algorithm [6].

2.1.2 Symmetric (Private Key) Model:

It is referred as conventional encryption. It is one of the cryptosystem forms in which same key is used for both encryption and decryption processes. Plaintext is turned into cipher text by the symmetric encryption through an encryption algorithm and a secret key. The plain text is restored using same key and a decryption algorithm. Symmetric cipher is made of two wide categories: block cipher and stream ciphers[7].

3. RELATED WORK

There are many works that related with our work, which presents the security of data in cloud computing as follow:

In 2012, Wentao Liu et al. [8] propose that the security issue of distributed computing is vital and it can keep the fast improvement of distributed computing. It presents some distributed computing frameworks and breaks down distributed computing security issue and its procedure as indicated by the distributed computing ideas and characters. The information protection and administration accessibility in distributed computing are the key security issue. Single security technique can't tackle the distributed computing security issue and numerous conventional and new advances and methodologies must be utilized together to protect the aggregate distributed computing framework.In 2013, Nikhilesh Pant et al. [9] present the procedures for cloud appropriation and cloud security appraisal to investigate potential security and consistence suggestions in cloud environment. They talks about in subtle element on how an association may continue for security and consistence appraisal amid the cloud calculation. Their methodology and ideas point by point in this paper would be valuable for associations that are included in the cloud reception process.In 2014, Liu X. [10] talks about distributed computing information security issues, including tile security of information transmission, stockpiling, security and administration of security. Concentrate on all inclusive information administration influence cloud security examination, and pointed out that a leap forward in the advancement of this distributed computing, attempt to list the comparing methodologies and long haul improvement heading,

4. RSA ALGORITHM

RSA algorithm is one of the frequently used asymmetric key cryptography algorithm that was developed by Ron Rivets, Adi Shamir, and Leonard Adelman in 1977. The naming was done based of the surnames of the developers. The algorithm can be

used for achieving both security as well as authentication of the information. Public-key cryptosystems are mostly used to secure the data during communication .RSA is an asymmetric key cryptography algorithm that uses public and a private key pair. Hence, the encryption of message are done at the sender end using the public key and the decryption are done at receiver end using the private key of receiver respectively. The reason of using RSA algorithm is the major problem in factorization of large integers. The security occurs due to the product of two large prime numbers during the algorithm implementation. The most compound part of RSA cryptography is the generation of public key and private key. Using Rabin–Miller primarily test algorithm ,two prime numbers are generated that are p and q. The link between private key and public key is provided by the two prime numbers. The key size is frequently expressed in bits. Figure (1) show the RSA algorithm architecture

4.1. Steps of RSA Algorithm

RSA algorithm involves three major steps during implementation. They are as

follows:

A. Generation of key

B. Encryption

C. Decryption.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 08, August 2024, pp: 507-512

Impact Factor: 5.725

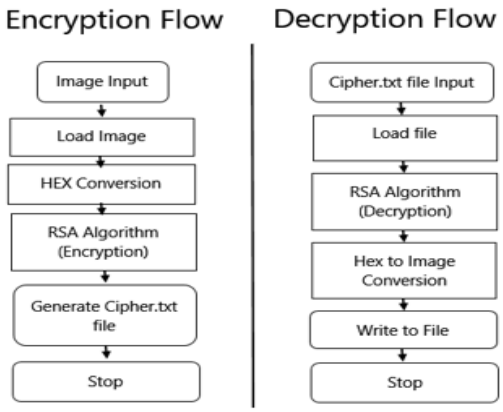


Figure (1) the RSA algorithm architecture

A. Key Generation

First stage of RSA algorithm is the key generation that involves public and private generation. As the name represents, public key is an open key that can be seen to everyone, and it is used to participate in encryption of messages Transmitting images are going through encryption using public key, and after that it can perform decryption via using private key. The keys of RSA algorithm can create using the subsequent steps,

1. First, we have to select the two different prime numbers that is p and q.

2. For safety, prime integers p and q should be selected with same bit-length. Prime integers are proficiently found by the primality testing.

3. Then, we have to calculate the value of n that is n = pq.

4. n is the modulus that is used for equally the public and private keys. Its length is known as key length that is usually stated in bits.

5. We have to compute Euler's to tient of n. $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1) = n - (p + q - 1)$; here, ϕ is Euler's toting function. This rate is kept private.

6. Then, we have to choose an integer e that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; i.e., e and $\phi(n)$ are coprime. e is out as key which kept public. e has a brief bit-length and slight Hamming weight outcomes in more effective encryption. However, much minor e values have been publicized to become less locked in some settings.

7. Determine d as $d \equiv e - 1 \pmod{\phi(n)}$, i.e., d which is the modular multiplicative inverse of e (modulo $\phi(n)$). This is performed as, solve d given by $d \cdot e \equiv 1 \pmod{\phi(n)}$. That is calculated using extended Euclidean algorithm.It uses the pseudo-code in the modular integers section; inputs a and n correspond to e and $\phi(n)$, respectively. 8. Evaluate the value of d which is kept as the private key.Public key involves the modulus of n and e. The private key has the modulus of n and d, and it kept secret. p, q, and $\phi(n)$ values are kept secret because these values can be used for calculating d.

B. Encryption

$c \equiv me \pmod{n}$_c = cipher text,m = plain text, e = public key, d = private key_

C. Decryption

$m \equiv cn \pmod{n}$_c = cipher text,m = plain text, e = public key, d = private key_

5. PROPOSED METHOD AND PERFORMANCE ANALYSIS

RSA algorithm uses discrete logarithm approach for implementation. Discrete we have used RSA algorithm in our research work for achieving image security. Since, RSA algorithm involves discrete logarithm approach and it is very difficult was used in many real life applications for information security, so we have used this algorithm was used for the security of information. The proposed image encryption technique is implemented by considering a random image as a key. The flow representation of the whole encryption and decryption process is depicted in Figure(1) .

5.2 Encryption

In encryption, the plain text content represented in the form of image is converted cypher text using another image as a secrete key. The picture can likewise be changed over to scrambled structure utilizing the random image as key and the resultant image after encryption is represented in Figure (2). The scrambled picture is then sent over an insecure channel to the receiver. At the receiver end, the scrambled picture is decoded using the private key of the receiver. The proposed image encryption technique is used for providing better security of information. Subsequent, to encoding information, objective-scrambled information was decoded with assistance of association called as unscrambling. The

resultant encrypted image are generated by applying the RSA algorithm between information image and the key image i.e. the binary equivalent of information image undergoes encryption with each pixel corresponding binary equivalent of key image in order to produce the encrypted image. .

5.3 Decryption

The resultant encrypted image undergoes decryption using the RSA algorithm. The resultant image after decryption is the same as that of the original image. In our research work, we have considered four different images out of three grayscale images and one color image for encryption and decryption using the RSA algorithm. The resultant encryption and decryption for each image using the traditional and proposed approaches are depicted in Figure(2) respectively.

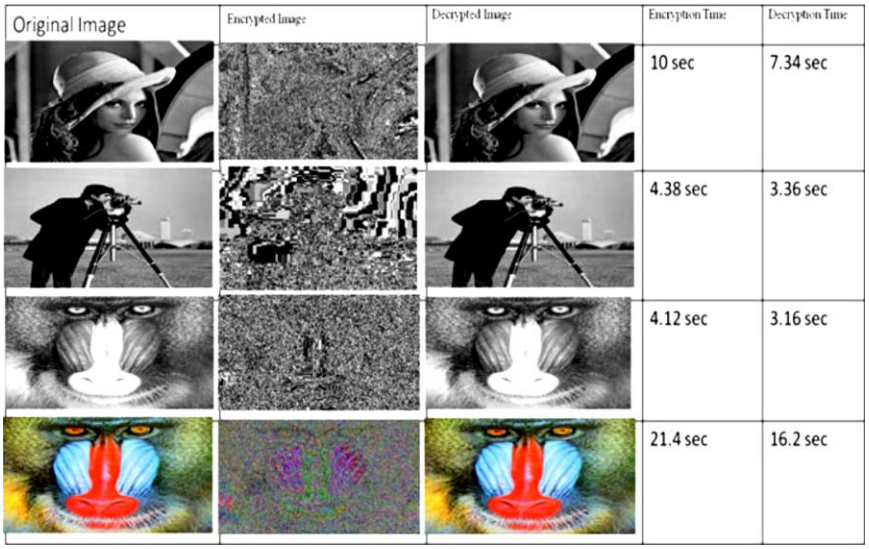
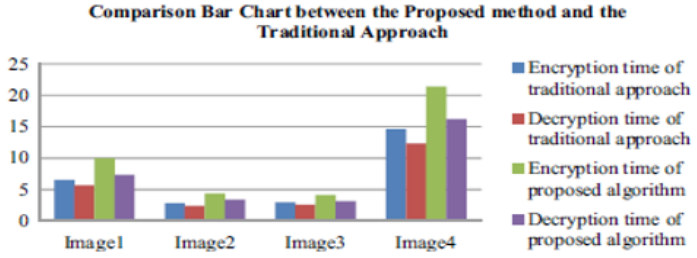


Figure (2) show Original image, the encryption image and decryption image in RSA algorithm

Table 1 Experimental result using the proposed method

	Encryption time of Traditional approach (s)	Decryption time of traditional approach (s)	Encryption time of proposed algorithm (s)	Decryption time of proposed algorithm (s)
Image1	6.56	5.66	10	7.34
Image2	2.81	2.38	4.38	3.36
Image3	2.95	2.57	4.12	3.16
Image4	14.6	12.3	21.4	16.2
Average time	6.73	5.72	7 9.975	7.515

The time required for different operations based on our proposed approach is represented in Table 1.It shows the calculated time values for both the algorithms. If we compare the average time of this traditional approach and proposed algorithm, then we will see that the average time of encryption and decryption is high, while using image as a key. So, it is more secure than the traditional approach. That it will take more time to encode and decode the information by an attackers, so it is more encore Figure(3). The calculated time for different activities during the algorithm implementation could be represented as:



Figure(3) Comparison bar chart

	Encryption time of Traditional approach (s)	Decryption time of traditional approach (s)	Encryption time of proposed algorithm (s)	Decryption time of proposed algorithm (s)
Image1	6.56	5.66	10	7.34
Image2	2.81	2.38	4.38	3.36
Image3	2.95	2.57	4.12	3.16
Image4	14.6	12.3	21.4	16.2
Average time	6.73	5.72	7 9.975	7.515

It represents the graphical data and comparison between two algorithms. In this bar chat, blue color bar shows the encryption time of traditional approach; red color bar shows the decryption time of traditional approach; green color bar shows encryption time of proposed algorithm, and navy blue color bar shows decryption time of our proposed algorithm. It shows that for every image, the time of encryption and decryption of proposed algorithm is higher than the traditional approach, so it will be more secured.

6. HISTOGRAM ANALYSIS

It is an effective way of comparing two images and thus illustrating the image quality. The Histogram plots of Original Image and the Encrypted Image should always be different while the histogram plots of the original and decrypted images should be the same . Figure (3) show a. Original image ,b. the encryption image and c . decryption image .

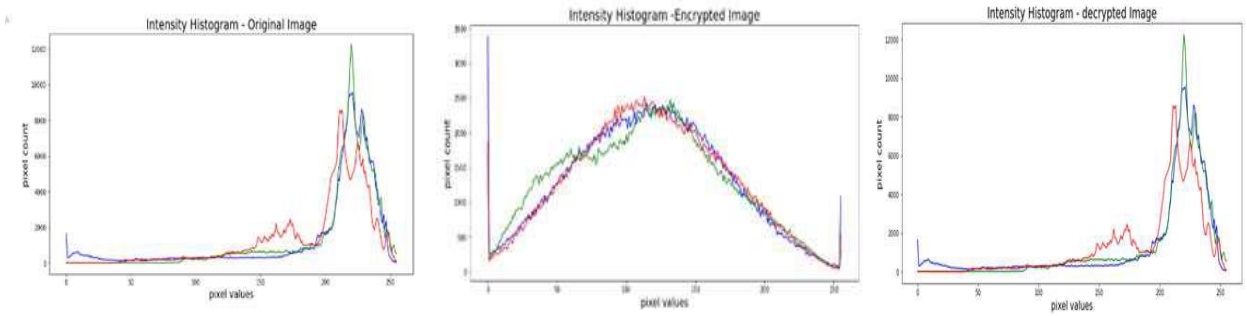


Figure (3) The Histogram plots of a. Original image , b. the encryption image c . decryption image

7. CONCLUSION

The asymmetric encryption algorithm of RSA makes encryption more secure and the receiver is not too afraid to give each sender a different key to ensure communication. And another advantage of the RSA algorithm is that the RSA algorithm is difficult to decipher because it involves the factorization of prime numbers that are difficult to factor. If in one way or another, the use of permutation or attempted piracy is able to get the decryption key is almost equal to the original key. In this paper we shown the overview of the RSA algorithm and also shown the obtained output results in the form of image encryption and decryption which is very useful to the digital image security purpose.

8. REFERENCES

[1] Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing. In 31st international conference on distributed computing systems (ICDCS) 2011 (pp. 383-92). IEEE.

[2] Yang Y. Towards multi-user private keyword search for cloud computing. In IEEE international conference on cloud computing (CLOUD) 2011 (pp. 758-9). IEEE.

[3] Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(5):847-59.

[4] Naqvi S, Michot A, Van de Borne M. Analyzing impact of scalability and heterogeneity on the performance of federated cloud security. In IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom) 2012 (pp. 1137-42). IEEE.

[5] Tianfield H. Security issues in cloud computing. In IEEE international conference on systems, man, and cybernetics (SMC) 2012 (pp. 1082-9). IEEE.

[6] Abuhussein A, Bedi H, Shiva S. Evaluating security and privacy in cloud computing services: A Stakeholder's perspective. In international conference for internet technology and secured transactions 2012 (pp. 388-95). IEEE.

[7] Zhao F, Li C, Liu CF. A cloud computing security solution based on fully homomorphic encryption. In 16th international conference on advanced communication technology (ICACT) 2014 (pp. 485-8). IEEE.

[8] Liu W. Research on cloud computing security problem and strategy. In international conference on consumer electronics, communications and networks (CECNet) 2012 (pp. 1216-9). IEEE.

[9] Pant N, Parappa S. Seeding the cloud in a secured way: cloud adoption and security compliance assessment methodologies. In IEEE international conference on software engineering and service science (ICSESS) 2013 (pp. 305-8). IEEE. [24] Liu X. Data security in cloud computing. In proceedings of the 2012 international conference on cybernetics and informatics 2014 (pp. 801-6). Springer New York.

[10] Yang F, Pan L, Xiong M, Tang S. Establishment of security levels in trusted cloud computing platforms. In green computing and communications (GreenCom), IEEE and internet of things (iThings/CPSCom), IEEE international conference on and IEEE Cyber, physical and social computing 2013 (pp. 2119-22). IEEE.

[11] Gupta A, Chourey V. Cloud computing: security threats & control strategy using tri-mechanism. In international conference on control, instrumentation, communication and computational technologies (ICCICCT) 2014 (pp. 309-16). IEEE.