International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 650-654 Jan 2019-June 2019 www.csjournals.com

A Novel Digital Image Encryption Method Based on RSA Algorithm

Aman Jain, Simran Sharma
Jaypee Institute of Information Technology, Noida

Abstract— With the development of production and applications for digital images, the safety of digital images has become very important in the modern world. The recent trend in digital imaging technology encryption is method to secure the digital images. The encryption is done by using the various algorithm, transformation and many more techniques to secure the digital image. In this paper, present a digital image encryption technique which is enhancing the security of digital image using the RSA Algorithm. Information is the currency of democracy Impermeability during transfer and storage become a problem in the field of data transmission. One of the most effective solutions for this growing problem is encryption. The aim of this paper has to secure the digital image using the RSA algorithm in the form of the image encryption.
Keywords: Cryptography, Decryption, Encryption, Image Encryption, RSA Algorithm.

I. INTRODUCTION

Since digital imaging plays an important role in multimedia technology, maintaining user privacy becomes even more important. To ensure such security and privacy for the user, it is very important to encrypt the image to protect against unauthorized access. Encryption of images and video is used in various fields, including Internet communications, multimedia systems, medical imaging, telemedicine and military communications. Colour images are transmitted and stored in large quantities via the Internet and wireless networks that use the rapid development of multimedia and network technologies. Cryptography has played an important role in security, and this is the battlefield for mathematicians and scientists from Shannon since 1949. Several cryptographic algorithms are now offered as AES, DES, RSA, IDEA, etc [5].

The image is the communication mode most used in different fields such as medical field, research field, industry, military area, etc. The important transfer of images will take place in an unsecured Internet network. Therefore, there is a need for appropriate security so that the image prevents access by the unauthorized person to important information. The advantage of the image is that it covers more multimedia data and needs protection. Cryptography is a type of image security method; It offers the secure method of transmitting and storing the image on the Internet. Security is the main concern of any system to maintain the integrity, confidentiality and authenticity of the image. Although cryptography is the efficient method, it also faces the problem of security if data with gray levels are more numerous [3].

II. IMAGE ENCRYPTION

Encryption is the study of techniques to guarantee the communication process between the sender and the receiver in the presence of third parties called "liabilities". Essentially, it is understood that the design of protocols based on mathematics, computer science and electrical engineering encrypt and decipher information in the form of data and images.
Modern cryptography can be classified broadly into two types:-

A. Symmetric key cryptography

In the form of encryption, there is only one key and the private key is used to encrypt and decrypt data between the sender and receiver.

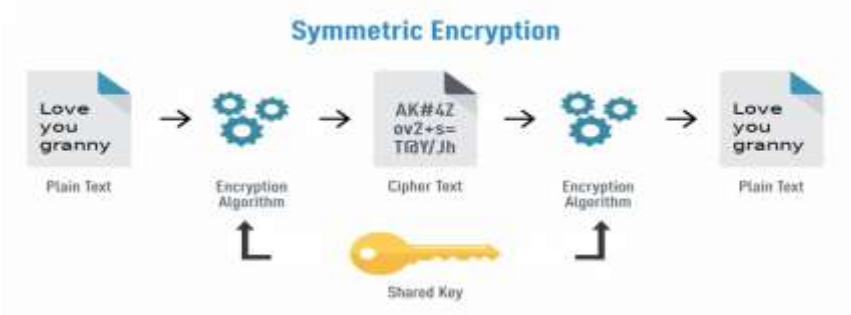


Figure 1 : Symmetric Key Cryptography

B. Asymmetric key cryptography

In this type of encryption, there are two types of keys: the public key and the private key. Both are used in encryption and decryption. The public key is available to everyone.

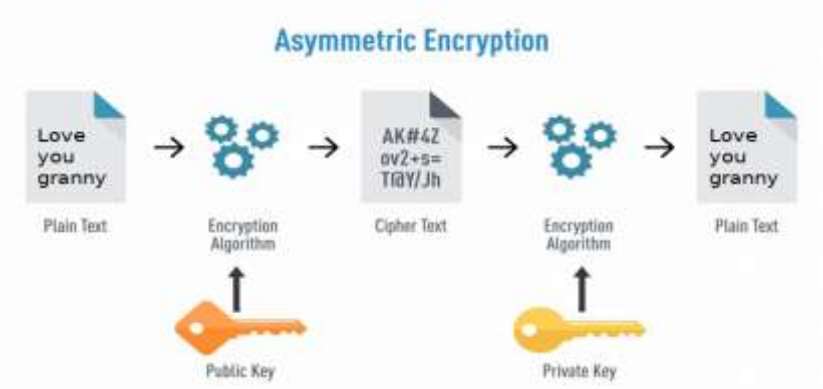
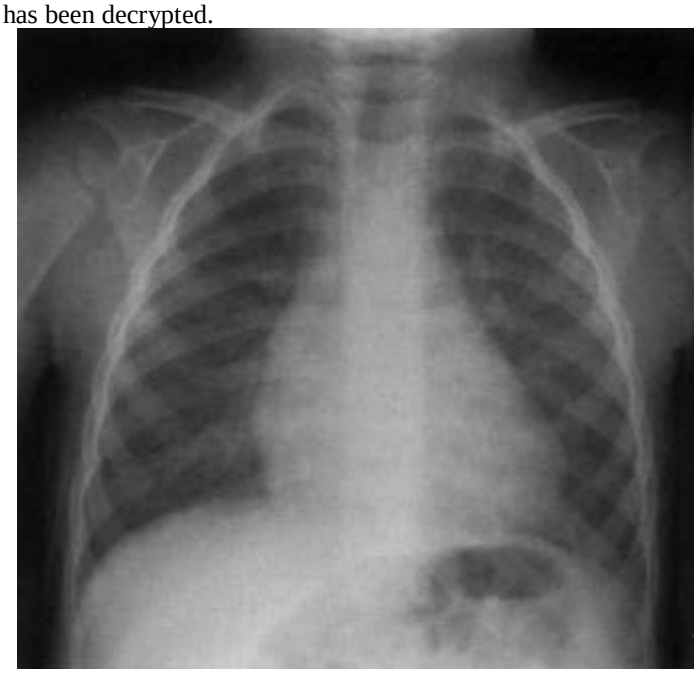


Figure 2: Asymmetric Key Cryptography

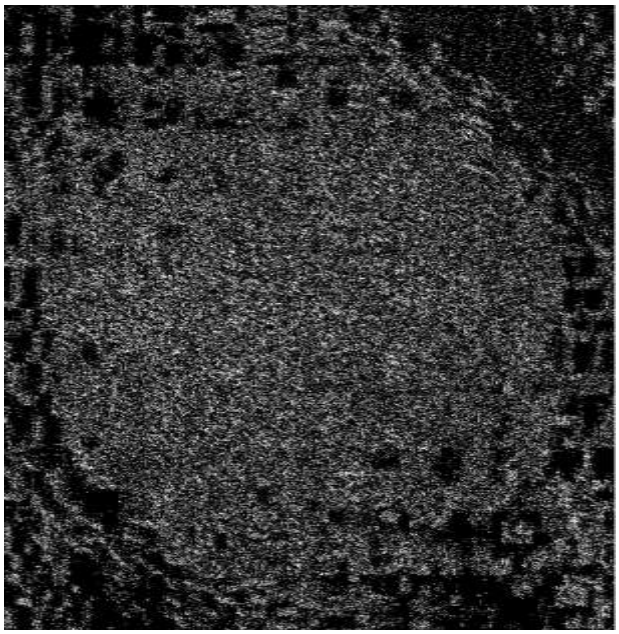
The encryption of the image is done to guarantee the safe transfer of images on the Internet. The encryption mechanism is widely used in this area of image / video transfer, since it does not provide access to unauthorized access. Encryption is also applicable in military communications and telemedicine. Up to the future point of view, the encryption has a greater scope. In the case of image security, the image contains large data, such as high frequency, large capacity and high pixel correlation. The techniques used in encryption can be considered as a tool to protect confidential data. Encryption is a mechanism that can be converted into encrypted or protected data, and can only be read by deciphering it. The process of reverse encryption is known as decryption, which uses a cryptographic key to decrypt the original data. Data encryption has become the best choice for all confidential data, including through the Internet, external networks or internal networks. Encryption is done by applying a mathematical function that generates a key later, and the key is used to obtain the encrypted data. Again, the mathematical key obtained is used for the original data. Security Manager is used to authenticate the user and accuracy in data security [8].

Image encryption is a technique used to hide data or secure image information. This is one of the most common methods that use secure image data. In this way, the image is encrypted and the encrypted image differs from the original image. The encrypted image shows no part of the original image. To obtain the original image from the encrypted image, it has been decrypted.



(a) Original Image

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 650-654 Jan 2019-June 2019 www.csjournals.com



(b) Encrypted Image

Figure 3: Image Encryption

III. RSA ALGORITHM

Public-key cryptography is also called asymmetric. It requires the use of a private key (a key that only its owner knows) and a public key (a key that both know). Public key cryptography is a fundamental technology and widely used throughout the world. It is the approach used by many cryptographic algorithms and commonly used for the distribution of software, financial transactions and in other critical security areas where it is important to protect against counterfeits and falsifications.

RSA is the most popular asymmetric digital image encryption algorithm. RSA (named for Rivets, Shamir and Adelman, who first described it publicly) is the first known algorithm for both signing and encryption, and was one of the first major advances in public-key cryptography. It uses a pair of keys, one of which is used to encrypt the digital image in such a way that it can only be verified with the other key of the pair [1].

The keys are generated through a common process, but cannot be generated in a viable manner among them. The security of RSA depends solely on finding the prime factors that are used in the process of encrypt and decrypt, the digital image and is based on the assumption that factoring a large number is difficult. "Multiplying two large prime numbers is a one-way function. It is easy to multiply the numbers to obtain a product, but it is extremely difficult to factor the product and retrieve the two large prime numbers that have been multiplied previously. it is known as a factoring problem. "

In this research, the security of the existing algorithm is improved whenever no one finds a way to solve this problem in a reasonable amount of time. RSA will be a secure encryption algorithm.

IV. MATHEMATICAL BACKGROUND OF RSA ALGORITHM

RSA (named for Rivest, Shamir and Adelman, who first described it publicly) is an algorithm for asymmetric cryptography. It is the first algorithm known to be suitable for signing and encryption, and it was one of the first great advances in public-key cryptography. It is widely believed that RSA is safe with sufficiently long passwords.

First find two prime numbers and generate a pair of keys using those two prime numbers.

- p and q are different cousins

$$N = \pi * \ \theta \qquad \_\_\_\_\_ (1)$$

- Find e, d such that:

$$e * d = 1 \bmod (p-1)(q-1) \qquad \_\_\_\_\_ (2)$$

$$\text{Private key: } = (n, d) \qquad \_\_\_\_\_ (3)$$

$$\text{Public key: } = (n, e) \qquad \_\_\_\_\_ (4)$$

Then, the encryption of the image and the decryption of the image are made using the key pair.

- Image Encryption:

$$S(m) = md \bmod n = S \qquad \_\_\_\_\_ (5)$$

- Image Decryption:

$$V(S) = \text{Mod } n = m \qquad \_\_\_\_\_ (6)$$

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 650-654 Jan 2019-June 2019 www.csjournals.com

V. DIGITAL IMAGE ENCRYPTION USING THE RSA ALGORITHM

The RSA is the one of the most popular algorithm which is used to be digital image security or digital image encryption purpose. The encryption is one of the best techniques to secure the data or image at the time of communication. In encrypted image no one can be see the original data or image which is in it, to see the original data or image we can use the decryption technique to get the original image from the encrypted image.
The different obtained simulations result is shown in the below which is done for the image encryption purpose using the RSA algorithm.

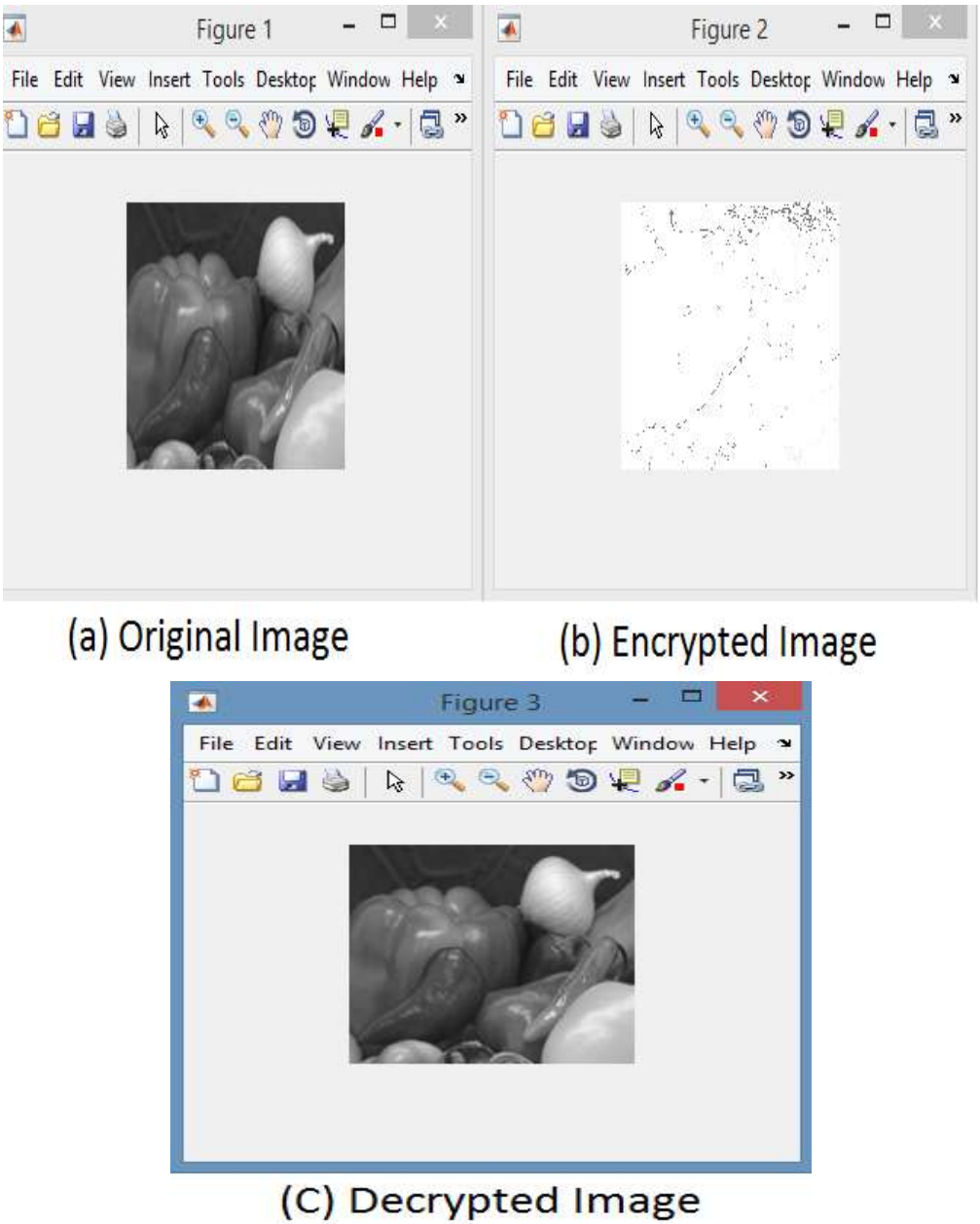


Figure 4 : (a) Original Image of Vegetable , (b) Encrypted Image of Vegetable USing RSA Algorithm, (c) Decrypted Image of Vegetable Using RSA Algorithm

VI. 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.

REFERENCES

1. Aniati Murni, "Image Processing", class handouts, Faculty of Computer Science, University of Indonesia, Jakarta, 2000.
2. Rohit Minni, Kaushal Sultania, Saurabh Mishra and Prof Durai Raj Vincent PM, " An Algorithm to Enhance Security in RSA" , IEEE 4th ICCCNT 2013, pp- 1-4, July 4-6, 2013.
3. Khalid Hamdnaalla1, Abubaker Wahaballal and Osman Wahballa1, " Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithm", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:13 No:04, pp-6-17, August 2013.
4. Rohit Minni, Kaushal Sultania, Saurabh Mishra and Prof Durai Raj Vincent PM, "An Algorithm to Enhance Security in RSA", IEEE 4th ICCCNT 2013, pp- 1-4, July 4-6, 2013.
5. Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, "Image Cryptography: A Survey towards its Growth", Advance in Electronic and Electric Engineering, Volume 4, Number 2, pp. 179-184, 2014.
6. Sangita A. Jaju and Santosh S. Chowhan, "A Modified RSA Algorithm to Enhance Security for Digital Signature", IEEE, pp-1-5, 2015.
7. Madhu B., Ganga Holi and Srikanta Murthy K., " An Overview of Image Security Techiques ", International Journal of Computer Applications, Volume 154 – No.6, pp- 37-46, November 2016.
8. Shankha Mukherjee, Shakya Chakrabarti, Souvik Sinha and Tamal Mukhopadhyay, " A meticulous implementation of RSA Algorithm using MATLAB for Image Encryption" , IEEE, pp- 1-6, 2017.
9. Shikha Mathur, Deepika Gupta, Vishal Goar and Manoj Kuri, "Analysis And Design Of Enhanced Rsa Algorithm To Improve The Security", 3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT 2017), pp-1-5, 2017.
10. Shankha Mukherjee, Shakya Chakrabarti, Souvik Sinha and Tamal Mukhopadhyay, "A meticulous implementation of RSA Algorithm using MATLAB for Image Encryption", IEEE, pp- 1-6, 2017.