AL-MUKHTAR JOURNAL OF ENGINEERING RESEARCH ISSN online: 2519-6839 // ISSN Print 2519-6820
Vol. 6, No. (1): 92-96 Available at mjer.omu.edu.ly
Received July 29, 2022, Accepted October 25, 2022, Published December, 2022 DOI: https://doi.org/10.54172/8a04cv25

Image Encryption using RSA Algorithm

Najeh Adam Farag

Department of Electrical Engineering, Faculty of Engineering, Omar Al-Mukhtar University, Libya, E-mail: najeh.adam@omu.edu.ly

Abstract

Today, it is necessary that effective encryption and decryption be utilized when transmitting data via the internet from one point to another in order to guard against unauthorized access. Image cryptography is a particular type of encryption technique that uses a key value to encrypt and decrypt the original message by hiding data within an image. There are very few algorithms, which makes computing complex, and it is challenging to crack a code to discover the original message. In this paper, the modified RSA encryption technique is used to transmit the image to the intended receiver with the highest level of confidentiality and secrecy. The modified RSA cryptosystem has been applied to both grey and color images using MATLAB software. Because of the complexity of factoring problem that converts positive integer into a product of two primes. Moreover, decrypting any encrypted images necessitates calculating a huge integer made up of the product of numerous large primes. The proposed technique was applied to encrypt images as the number of primes increases, which is more secure than the original RSA cryptosystem. The results shows that, using the modified RSA cryptosystem is more resistant to any attacks in the transmission of images in all agencies in the information technology era.

الملخص العربي

يقودنا ظهور التكنولوجيا الرقمية إلى ضرورة وجود مستوى عال من الأمان أثناء نقل الصورة الرقمية عبر قناة اتصال غير موثوقة. لهذا ، يعد التشفير أحد أفضل الطرق لضمان سرية وسلامة البيانات السرية. الهدف الورقة هو إرسال الصورة إلى جهاز الاستقبال المقصود بمنتهى السرية باستخدام خوارزمية التشفير **RSA**. نظرًا لأن نظام التشفير **RSA** هو نظام تشفير آمن جيدًا ، فإننا نستخدم **MATLAB** لتطبيق نظام التشفير هذا على الصور الرمادية والملونة. أمان **RSA** يعتمد على صعوبة مشكلة العوملة ، والتي تتمثل في تحليل عدد صحيح موجب في منتج مكون من اثنين من الأعداد الأولية ، فنحن نطبق نظام التشفير هذا على الصور مع زيادة عدد الأعداد الأولية. هذا يعطي نظام تشفير **RSA** المعدل أمانًا أعلى من نظام تشفير **RSA** ، لأن فك تشفير أي صور مشفرة يتطلب تحليل عدد صحيح كبير يتكون من ناتج ضرب أعداد أولية كبيرة ، ويتطلب معرفة حجم الكتل التي يتم تشكيلها من مصفوفة بسيطة. لذلك فإن طريقة تشفير وفك تشفير الصور باستخدام نظام التشفير **RSA** أكثر مناعة ضد أي هجمات في نقل الصور في جميع الوكالات في عصر تقنية المعلومات.

Keywords: Cryptography, Decryption, Encryption, Image Encryption, RSA Algorithm

Introduction

The importance of digital imagery in multimedia technologies makes it even more crucial to protect user privacy. It is crucial to encrypt the image in order to safeguard the user's security and privacy and prevent illegal access. Several industries, including Internet communications, multimedia systems, medical imaging, telemedicine ,and military communications, use picture and video encryption. Through the Internet and wireless networks, which make advantage of the quickly evolving multimedia and network technologies, color images are transmitted and stored in vast amounts. Security benefits of cryptography, and Shannon mathematicians and scientists have fought on this front since 1949. AES, DES, RSA, IDEA, and other cryptographic methods are now available [3]. The RSA cryptosystem was created by Rivest, Shamir, and Adleman in 1978 [3]. Since factoring n takes millions of years, it is a mathematical conjecture that the security of the modulo n into two huge prime integers determines the security of the RSA cryptosystem. However, since images are highly clear and visible, it is crucial and necessary to encrypt them in a way that renders them invisible before they are shared between individuals. To encrypt an image, Chandel and Patel in [1] split a color image into parts, then applied the RSA encryption technique to the split data. The intended recipient will then use a corresponding private key to perform the reversed procedure to decode and join all of the split data. They also used two critical security measures, one for data splitting and the other for encryption. Urbana Ivy, on the other hand, altered the RSA cryptosystem based on 'n' prime numbers in [2] B.Persis to boost its security, but he did not use it for image encryption. So, in this paper, we suggest a tweak to the RSA cryptosystem that encrypts both gray and color photos, expanding the number of primes in R that is MATLAB software-programmed.

RSA cryptosystem

In 1977[4], Ron Rivest, Adi Shamir, and Leonard Adleman created the RSA algorithm. RSA employs two keys—public and private—because it is an asymmetric key cipher. A reflection of a signal The decryption procedure uses the private key, while the encryption process uses the public key. Three major steps make up the RSA algorithm [1]:

1. Key Generation: The first phase of the RSA algorithm is key generation [5]. Since we already learned that the RSA algorithm employs two keys, we must calculate both keys. Four easy steps are involved in the key generation in RSA:

i. First, select two different prime numbers, p and q, and then compute $R = p \times q$.

ii. Second, is to find the Euler's function

$\varphi(R) = \varphi(pq) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$

iii. Third ,is to select e in such a way that

$1 < e > \varphi(R)$ and GCD$(e, \varphi(R)) = 1$ where

(e,R) is our public key

iv. Fourth , finding d in such a way that $ed = 1 \bmod \varphi(R)$where d is the secret key.

2. Encryption: By using the public key and the following formula, the sender encrypts the original text::

$X: E(X) = Y \equiv Xe \pmod R$

Where X isplain text

3. Decryption :The receiver decrypts the cipher text obtained through encryption using the private key and the formula:

$D(Y) = X \equiv (Y)d \pmod R$

Where Y is cipher text ..

Image Encryption using Modified RSA

In order to protect the privacy of the original image among users, an image encryption technology transforms a readable image into an image that is difficult to interpret. In other words, no one could access the original image's content without the decryption key. Every asymmetric cryptosystem includes separate public and private keys for each recipient. While the private key of RSA needs to be kept a secret, the public key of RSA is used in the encryption process and can be made public. The decryption process uses the private key. By constructing the modulo R of numerous unique large prime numbers and turning the image into a matrix, this approach focuses on the cryptosystem over images using MATLAB. The matrix is then divided into 2 x 2, 4 x 4, 8 x 8, or n x m sub-blocks. Then, for each and every sub block, we use modified RSA encryption and decryption algorithms [7].

key-generation of RSA [2]:

-To create the expression $(R = p*q*f \ldots *r)$,choose large prime numbers$(p, q, f, \ldots, r)$.

- Determine $\varphi(R) = (p-1)*(q-1)*(f-1)*\ldots*(r-1)$
- Select (e) such that $(1 < e < \varphi(R))$
- Find d such that $(e*d \equiv 1 \pmod{\varphi(R)})$
- (e, R) as the public key
- Keep (d) as the secret key.

Image Encryption

1: IRead the plain image into the appropriate matrix (call it w). w is plain image

2: Divide block w into a sub block ($i * i$) call it S_p. S_p is sub block of w

3: Reconstruct each sub block into a vector ($1, i * i$) and call it (u)

4: Determine $C = u^e \pmod R$ (by computing element by element)

5: Reconstruct each into sub block ($i * i$) that is indicated by S_C.

6: Construct the cipher image by assembling the sub blocks S_C in such a way that each sub block S_C corresponds to a subblockS_P in the plain image.

Image Decryption

1: Read the cipher image into the appropriate matrix (call it *cr2*)

2: Divide into sub block ($i * i$) call it S_{C1}. 3: Reconstruct each sub block into a vector ($1, i * i$) and call it (u_2)

4: Apply the decryption algorithm $P_d = (u_2)^e \pmod R$ over u_2(by computing element by element)

5: Reconstruct each P_{di} to sub block ($i * i$) that is indicated by S_d.

6: Construct the cipher image by assembling the S_d sub blocks so that each S_d sub block is the corresponding sub block to S_{c1} in the cipher image.

Histogram analysis

The image histogram is a graph that shows how many pixels have an intensity value. The horizontal axis of the graph represents intensity values, while the vertical axis of the graph represents the number of pixels with that intensity value. There will be three graphs for each color in a color image. Image histogram analysis is a simple method for determining the quality of an encryption algorithm. A good encryption algorithm will produce an encrypted image with a uniformly distributed histogram. Figure 1 [6] depicts histograms of the original image and encrypted images using the RSA algorithm. The histogram of an RSA encrypted image is not evenly distributed.

PSNR

PSNR is the peak signal to noise ratio of an original image compared to a compressed or reconstructed image. It is a comparison of the two image quality. For two similar images, the PSNR value will be very high, and vice versa. Two identical images, for example, will have a PSNR value of infinity, while two completely different images will have a very low PSNR value. To calculate the PSNR, first calculate the MSE (Mean Squared Error).

An image's MSE is defined as

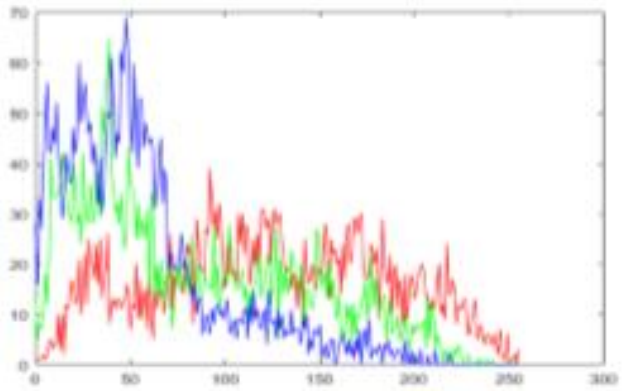
$$MSE = \frac{\sum x,y[I_{1(x,y)} - I_{2(x,y)}]^2}{x \times y} \quad (1)$$

x is the number of rows and y is the number of columns in the two images.

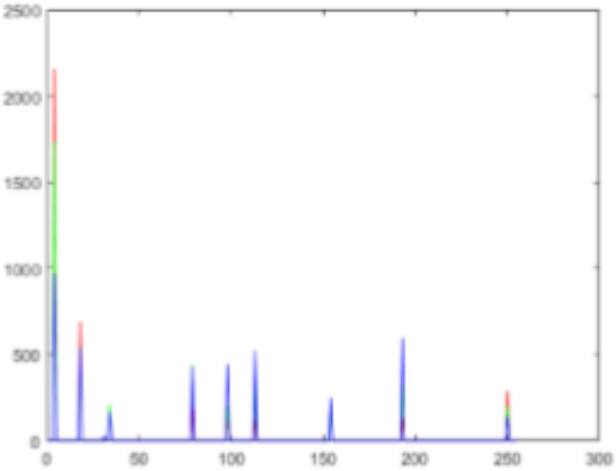
PSNR of an image is defined as

$$PSNR = 10 \log_{10}(\frac{R^2}{MSE}) \quad (2)$$

Figure 2 is a flowchart that describes the process of encryption and decryption



(a) Original Color Image



(b) RSA Encrypted color image

Fig.1 Histogram of Original and encrypted images

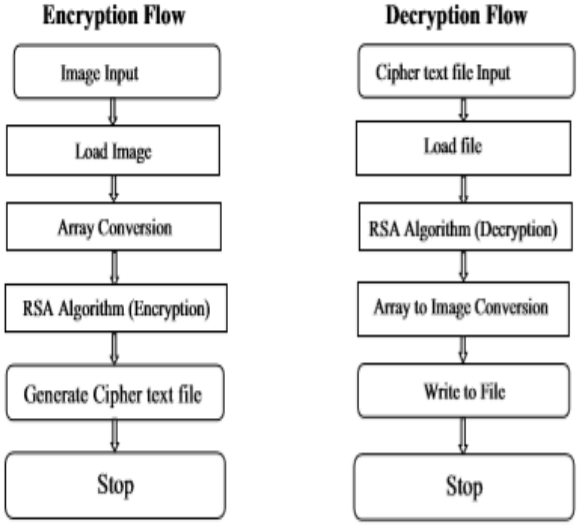


Fig. 2 Encryption and Decryption flow

Simulation Results

We used MATLAB software to digitize the image in this paper. First, we obtain the image's corresponding matrix. The corresponding matrix would then be encrypted using the RSA cryptosystem's encryption algorithm and three large prime numbers. The results show that the original images (color and gray) can be easily encrypted and decrypted with very good accuracy ,using MATLAB because the decryption process of an image in MATLAB is very smooth and the decrypted image looks exactly like the original image without any noise. One important note is that the image should be of the same dimension (n x n image) to facilitate the partitioning of the corresponding matrix into sub blocks.

This new approach proved to be far more secure than the previously mentioned RSA cryptosystem. Furthermore, it encrypts any grayscale or color image, resulting in an unintelligible image. This new method has very high accuracy standards when using the MATLAB program, as shown below:

PSNR (for both colored and gray images) = ∞ MSE (for both colored and gray images) =0 RMSE (for both colored and gray images) = 0

The following shows how applied this method on gray and color images using MATLAB:

Gray Image Encryption Operation

1-Input the public key such as
(e, R=$p.q.r$) = (23, 1463).
2-Read the original image (See Figure 1).
3- Obtain the encrypted image (See Figure 2).

Gray Image Decryption Operation

1- Input the receiver's private key
(d, R) = (47, 1463).
2- Read the encrypted image (See Figure 2)
3- Obtain the decrypted image (See Figure 3)

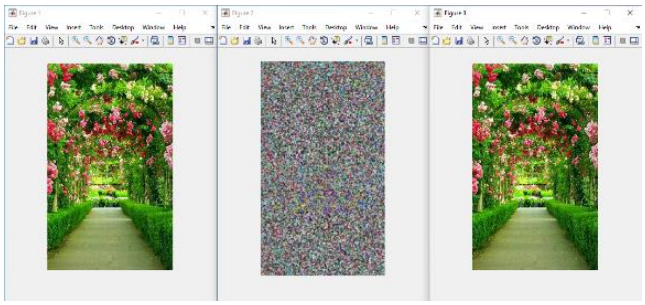
Color Image Encryption Operation

1- Input the receiver's public key such as
(e, R=$p.q.r$) = (23, 1463).
2- Read the original image (See Figure 4).
3- Obtain the encrypted image (See Figure 5)

Color Image Decryption Operation

1- Input the receiver's private key
(d, R) = (47, 1463).
2- Read the encrypted image (See Figure 5)
3- Obtain the decrypted image (See Figure 6)

The following shows figures for images:



(a) (b) (c)

Fig3. (a)Original color image (b) Encrypted color image (c) Decrypted color image.

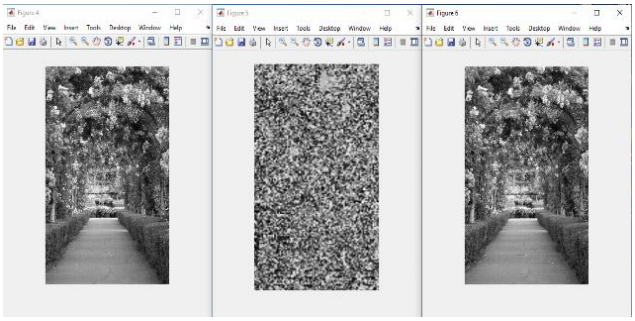


Fig4. (a)Original gray image (b) Encrypted gray image (c) Decrypted gray image.

Conclusions

In this paper, modified RSA was used to encrypt images, which is an asymmetric system based on the number of primes used with the help of the MATLAB program. Based on the obtained results, it can be noted that the modified RSA cryptosystem is a more secure encryption method. In addition to security, no data is lost in the decrypted images because the decrypted grayscale or color image is identical to the corresponding original image. Furthermore, the decryption is more difficult due to the factorization of difficult-to-factor prime numbers. A Modified Image Encryption Method in the Modified RSA Cryptosystem Key Anyone other than the creator, who is the receiver, must factor R to n chosen primes to find the private key, which is nearly impossible. As a result of this , we now have a new and secure strategy for encrypting any gray

or color image using the modified RSA cryptosystem programmed by MATLAB, and we have the confidence to transmit these images over any network, even if it is not very secure.

References

[1] Kaliski, B. The Mathematics of the RSA Public-Key Cryptosystem.RSA Laboratories, 2006.

[2] Ivy, B. P. U., & Kumar, P. M. M. A modified RSA cryptosystem based on ‘n’prime numbers. International Journal of Engineering and Computer Science ISSN, pp. 2319-7242, 2012.

[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] Rosen, K.H., Elementary Number Theory and Its Applications. 5th Edn., United State of America, Boston, 2005.

[5] H. Wang, Z. Song, X. Niu and Q. Ding, "Key generation research of RSA public cryptosystem and Matlab implement," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, Nangang, 2013.

[6] Chandel, G. S., & Patel, P. Image Encryption with RSA and RGB randomized Histograms. Image, 3(5), 2014.

[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.