Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 4 (2016), pp. 3631-3640
© Research India Publications
http://www.ripublication.com/gjpam.htm

A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB

Karrar Dheiaa Mohammed AlSabti [1] and Hayder Raheem Hashim [2]

[1&2]Faculty Of Computer Science And Mathematics, University Of Kufa, Iraq.

Abstract

The need of making important information that is being exchanged between participants through unsecure websites has intersted cryptoligists to create and modify some secure cryptosytems to prevent these information from getting hacked or cracked.In this paper, a particular strategy in thepublic key cryptosystem called RSA Cryptosystem is presented to be applied over gray and color images with the help of MATLAB Program. Since the RSA cryptosystem is a well-known secure cryptosystem, we use MATLAB to apply this cryptosystem over gray and color images. Moreover, that would be generating two algorithms for the encryption and decryption procedures. These algorithms can be applied over the plain image and cipher image after reading them in the matrices forms. However, the image is partitioned into blocks that are n x m matrices. Since the RSA cryptosystem is a secure public key cryptosystem since its security based on the difficulty of the factoring problem, which is factoring a positive integer R into a product of two primes, we apply this cryptosystem over images using MATLAB with increasing the number of the primes in R. This gives the modified RSA cryptosystem has a higher security than the RSA cryptosystem, because decrypting any encrypted images requires factoring the large integer composed of the product of many large primes, and it requires knowing the size of the blocks that are formed from plain matrix. Therefore, this approach of encrypting and decrypting images using RSA cryptosystem with some modifications more immune against any attacks in the transmission of images in all agencies in the era of the information technology.

Keywords: Cryptography, Public key cryptosystem, RSA cryptosystem, color and gray images, MATLAB.

1. INTRODUCTION

Cryptography has been interested people for long time especially with advent of electronic messaging, information technology and electronic banking. Traditionally, the need of exchanging information secretly in the communication has occurred in diplomacy and military affairs. Therefore, cryptography has become an important issue with coming of the electronic communication [4]. Indeed, there are two kinds of cryptosystem, which are the symmetric cryptosystems and the asymmetric cryptosystems. The symmetric cryptography requires a single key used the encryption and decryption processes. However, in the public key cryptography or asymmetric cryptography, there are two different keys in the encryption and decryption processes. One key is used in the encryption procedure and should be announced publicly, and the other is the corresponding private key that is used in the decryption procedure and should be kept secret by each person. There are many examples of the public key cryptography such as RSA cryptosystem, Hellman cryptosystem and ElGamal cryptosystem. Rivest, Shamir, and Adleman invented the RSA cryptosystem in 1978[3].The security of RSA cryptosystem depends on the security of the modulo n into two large prime numbers, and this is a conjecture in mathematics since factoring n requires thousands of years. On the other hand, images are very clear and visible things, so encrypting them in a way that makes them invisible before they are exchanged between people is really important and needed. However, in [1] Chandel and Patel used RSA and RGB in encrypting image by splitting a color image into parts, then apply the RSA encryption algorithm on the split data. Then, the intended receiver will decrypt and join all the split data by applying the reversed technique with the help of a corresponding private key. In addition, they applied two key securities; first for splitting data and second for encryption procedure. On the other hand, *in [2] B.Persis Urbana Ivy* modified the RSA cryptosystem based on ‘n’ prime numbers to increase its security, but he did not apply it in Image encryption. Therefore, in this paper, we propose a way to encrypt gray and color images using RSA cryptosystem with some modification by increasing the number of the primes in R programmed by MATLAB software.

2. RSA CRYPTOSYSTEM

The RSA cryptosystem is a public key cryptosystem, invented by three cryptologists who are Ron Rivest, Adi Shamir, and Len Adleman in 1970s [4] . The RSA is used for providing privacy, ensuring authenticity of digital data, electronic credit and debit cards payment systems, and commercial systems such as Web servers and browsers to secure Web traffic. Therefore, RSA is used in many applications where the security of digital data in the concern [5]. The RSA cryptosystem has two corresponding keys that are a public key and a private key. The public key can be announced publicly and is used for encrypting a plaintext or image. However, the corresponding secret key will be used to decrypt the cipher text [6]. The RSA's keys are generated as the following [1]:

- Each person chooses two large prime numbers p and q to form R=pq.
- Find the Euler's phi-function $\varphi(R) = \varphi(pq) = \varphi(p) \varphi (q)=(p-1)(q-1)$.

- Everyone chooses two positive integers **e** and **d** such that **d** is an inverse of **e** modulo φ(R).
- Everyone announces the pair (e, R) to be their public key and keeps is the pair (d, R) secret, which is their private key.

2.1.The encryption process for the RSA cryptosystem is as the following[7]:

- The intended receiver's public key (e, R) is used by a sender.
- To encrypt a plaintext that could be a message or an image, the sender translates the letters into their numerical equivalents (if needed) and then forms plaintext blocks, X, such that a nonnegative integer X less than R.
- Sender uses the following encryption algorithm to encrypt X: $E(X) = Y \equiv X^e$ (mod R). This Y is the corresponding ciphertext to X and is sent to the receiver.

2.2.The decryption process for the RSA cryptosystem is as the following[7]:

- To decrypt the ciphertext block Y, the following decryption algorithm is applied on every block Y: $D(Y)=X\equiv (Y)^d$ (mod R).

2.3.The security of the RSA cryptosystem:

The security of the RSA cryptosystem relies on the integer factorization problem to find the secret key (**d**, R), which many cryptologists try to recover [3]. If anyone can get the factors p and q of R, then it is so easy to find φ (R) and **d** and since **e** is known. Many studies showed that if R is a large composite number, then it is hard to obtain the prime factors of R. Thus, hacking or cracking the RSA cryptosystem by factoring R would not be easy, and it is a conjecture in mathematics. Nevertheless, there might other ways to obtain d. It can be obtained by finding φ(R) from R, such that find φ(R)= φ(pq)= φ(p) φ(q)=(p-1)(q-1). Then p and q , that factorize R, can be found easily. Note that finding φ(R) is not easier that factoring R. Moreover, when p and q both have approximately 300 decimal digits, R=pq has approximately about 600 decimal digits. Using the fastest factorization algorithm to factor an integer of this size, more than millions of years of computer time are required to factor it[4].

3. THE PROPOSED APPROACH FOR IMAGE ENCRYPTION USING MATLAB

An Image encryption technique converts a readable image to an image that is not easy to understand; to keep the original image confidential between users. In other word, without knowing the decrypting key, no one can get the content of the original image. Every single asymmetric cryptosystem has public and private keys that are unique for every recipient. The public key of the RSA is used in the encryption procedure and can be published to everyone, while the private key of the RSA must be kept secret. The private key is used in the decryption procedure. However, the RSA cryptosystem is also used in encrypting and decrypting messages, e-mails, software, and files, we propose to use MATLAB over encrypting and decrypting gray and color images using the RSA cryptosystem with especial techniques. These techniques focus on applying one of the most well-known asymmetric cryptosystems ,which is the RSA cryptosystem over images using MATLAB by composing the modulo R of many distinct large prime numbers and converting the image into a matrix, then dividing this matrix into 2 x 2, 4 x 4, 8 x 8, or n x m sub-blocks. Then, we apply modified RSA encryption and decryption algorithms over every single sub block.

3.1.The following shows the key-generation process of the modified RSA [2]:

- Select k large prime numbers (p, q, f,…., r) to form (R =p*q*f…*r).
- Compute $t = (p-1) *(q-1)*(f -1) *\ldots* (r-1)$
- Choose (e) such that ($1 < e < t$)
- Find d such that ($e*d \equiv 1 (\bmod t)$)
- Announce (e, n) as the public key
- Keep (d) as the secret key.

3.2.The image encryption procedure as the following :

Step 1: Read the plain image into its corresponding matrix (call it W).

Step 2: Partition W into sub block (i * i) call it S_P.

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

Step 4: Compute $C= u^e (\bmod R)$ (by computing element by element such that $Ci= u_i^e (\bmod R)$)

Step 5: Reshape each Cito sub block (i * i) that is denoted by $S_{C.}$

Step 6: Construct the cipher image gathering the sub blocks S_C such that every sub block S_C is the corresponding sub block to S_P in the plain image.

3.3.The image decryption procedure as the following:

Step 1: Read the cipher image into its corresponding matrix (call it cr_2)

Step 2: Divide into sub block (i * i) call it S_{C1}.

Step 3: Reshape each sub block into a vector (1, i * i) and call it (u_2)

Step 4: Apply the decryption algorithm $P_d= (u_2)^e (\bmod n)$ over u_2(by computing element by element
such that $P_{di}= u_{2i}^d (\bmod n)$

Step 5: Reshape each P_{di} to sub block (i * i) that is denoted by $S_{d.}$

Step 6: Construct the decrypted image gathering the sub blocks S_d such that every sub block S_d is the corresponding sub block to S_{c1} in the cipher image.

4. APPLICATIONS AND RESULTS

In this paper, we have digitized some well-known test images and a local taken image using MATLAB software. First, we obtain the corresponding matrix of a taken. Then, we would use the encryption algorithm of RSA cryptosystem with three large prime numbers to encrypt the corresponding matrix. The result shows that the original images (color and gray scale) can be encrypted and decrypted easily using MATLAB with very good accuracy since the decryption process of an image goes very smooth in MATLAB and the decrypted image comes exactly as the original image without any noise. One of the important notes is the image should be with the same dimension (n x n image) to make the partitioning of the corresponding matrix to sub blocks easier.

It turned out that this new approach is much more secure than the mentioned RSA cryptosystem. In addition, it encrypts any gray or color image to produce an unintelligible image. This new method has very good accuracy standards using MATLAB Program as the following:

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 we applied this approach on gray and color images using MATLAB:

1-Gray Images:

1.1- Encryption Procedure:[By the sender]

Step 1: Input the receiver's public key such as (e, R=p.q.r) = (13, 1771).

Step 2: Read the original image (See Figure 1).

Step 3: Produce the encrypted image (See Figure 2).

1.2- Decryption Procedure:[By the receiver]

Step1: Input the receiver's private key (d, R) = (1117, 1771).

Step 2: Read the encrypted image (See Figure 2)

Step 3: Produce the decrypted image (See Figure 3)

2-Color Images:

2.1.Encryption Procedure:[By the sender]

Step 1: Input the receiver's public key such as (e, R=p.q.r) = (13, 1771).

Step 2: Read the original image (See Figure 4).

Step 3: Obtain the encrypted image (See Figure 5).

2.2.Decryption Procedure:[By the receiver]

Step1: Input the receiver's private key (d, R) = (1117, 1771).

Step 2: Read the encrypted image (See Figure 5)

Step 3: Obtain the decrypted image (See Figure 6)

The following shows this new approach procedures' figures over two chosen images:

Original image	Encrypted image	Decrypted image
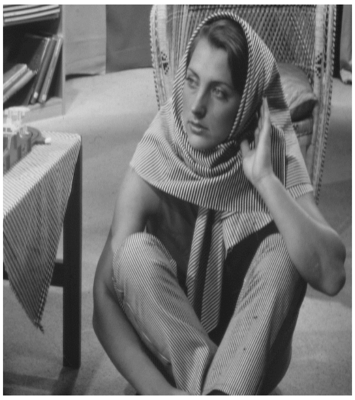	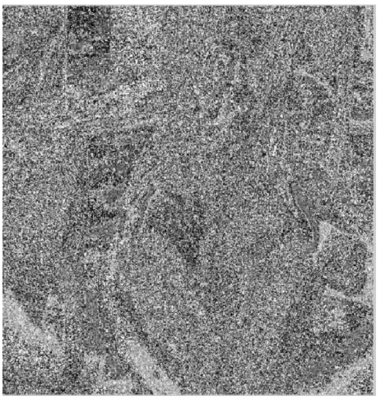	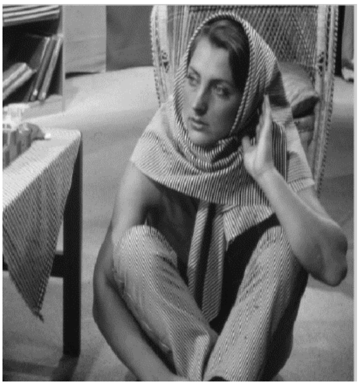
Figure 1	**Figure 2**	**Figure 3**
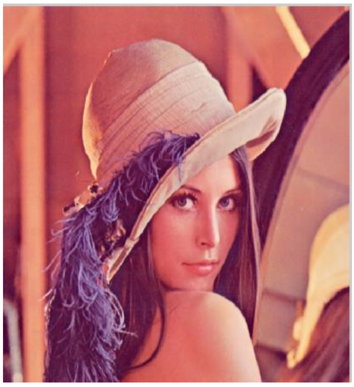	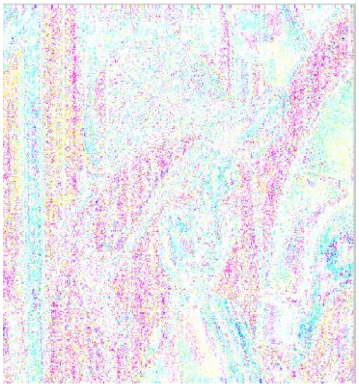	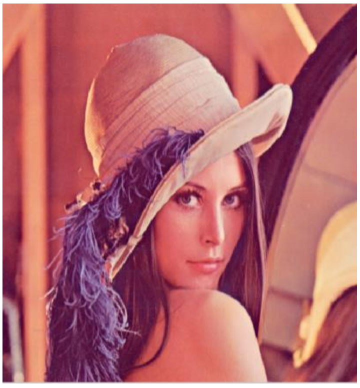
Figure 4	**Figure 5**	**Figure 6**

5. CONCLUSION

This paper proposes a new approach image encryption using the asymmetric cryptosystem, a modified RSA cryptosystem based on the number of the used prime numbers, with help of MATLAB program. Since MATLAB program is used to perform the encryption and decryption procedures. However, the original RSA has been applied in image encryption, this new approach gives a better security for image encryption since the modified RSA cryptosystem based on ‘n’ primes is much more secure than the original RSA cryptosystem as it is published by B.Persis Urbana Ivy. In addition to the security, there is no data lost in the decrypted images since the decrypted gray or color image comes out to be exactly as the corresponding original image. Moreover, we see that the decrypted image is totally different from the original image, so that no one can determine the original without knowing the private key. Finding the private key by anyone other than the creator, who is the receiver, she must factor R to **n** chosen primes, which is quiet impossible. Therefore, this approach produces a new and secure strategy to encrypt any gray or color image using the modified RSA cryptosystem programmed by MATLAB and gives us the confidence to transmit these images thru any network even if it was not very secure.

6. MATLAB ENCRYPTION AND DECRYPTION ALGORITHMS

```
clc
clearall
p= input('first prime number =');
q= input('second prime number =');
r= input('third prime number =');
nn=p*q*r
e=7;
dd=943;
w=imread('barbara512.bmp');
a=double(w);
n=input ('value of n =');
m=input ('value of m =');
d=n;
k=n;
for i=1:n:512
for j=1:n:512
    x=1;
for c=i:d
      y=1;
for r=j:k
s(x,y)=a(c,r);
ss(y,x)=s(x,y);
      y=y+1;
end
    x=x+1;
end
```

```
 u=reshape(ss,1,n*n)
 [o m]=size(u);
for xx=1:m
p = java.math.BigDecimal(1);
for ii = 1:e
  p = p.multiply(java.math.BigDecimal(u(xx)));
end
 p=p.remainder(java.math.BigDecimal(nn));
 y=p.intValue();
cr(xx)=y;
p2 = java.math.BigDecimal(1);
for iii = 1:dd
    p2 = p2.multiply(p);
end
p2=p2.remainder(java.math.BigDecimal(nn));
 x=p2.intValue();
sr(xx)=x;
end
cr
sr
cr1=reshape(cr,n,n);
sr1=reshape(sr,n,n);
for ii=1:n
forjj= 1:n
cr3(ii,jj)=cr1(jj,ii);
sr3(ii,jj)=sr1(jj,ii);
end
end
      x=1;
for c1=i:d
           y=1;
for r1=j:k
```

```
cr2(c1,r1)=cr3(x,y);
sr2(c1,r1)=sr3(x,y);
        y=y+1;
end
     x=x+1;
end
     k=k+n;
end
   d=d+n;
   k=n;
end
psnr=mselossy(a,sr2);
psnr
figure
imshow(cr2,[]);
figure
imshow(sr2,[]);
```

ACKNOWLEDGMENT

We are very thankful to our colleagues, at the Faculty of Computer Science and Mathematics, who have encouraged us to make this paper as an unforgettable experience in the scientific research.

REFERENCES

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

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

[3] Sklavos, N. and Zhang, X.,.2007. Wireless Security and Cryptography: Specification and Implementations. United States of America on, Taylor & Francis Group, LLC, ISBN-13:978-0-8493-8771-5.

[4] Rosen, K.H., 2005. Elementary Number Theory and Its Applications. 5th Edn., United State of America, Boston, ISBN-10: 0201870738.

[5] Boneh, D., 1999. Twenty years of attacks on the RSA cryptosystem. Notices of the AMS, 46(2), 203- 213.

[6] Hoffstein, J., Pipher, J. and Silverman, J.H.(2008). An Introduction to Mathematical Cryptography. Springer, Science +Business, Media, LLC, 233, USA, New York.

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