International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229431

Digital Image Encryption and Decryption based on RSA Algorithm

Radhakrishna M [1], Shridevi KS [2], Sowmya BS [3], Sushmitha TJ [4]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore, Karnataka, India

[2,3,4] Student, Department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore, Karnataka, India

Article Info
Volume 9, Issue 4

Page Number : 168-173

Publication Issue :
July-August-2022

Article History
Accepted : 05 July 2022
Published: 20 July 2022

ABSTRACT

Digital images are crucial in many areas, including online communication, multimedia systems, medical imaging, and military communications. Color images are being stored and transmitted over the internet and wireless networks in large amounts and thus it is necessary to protect them from any unauthorized user access. Cryptography is the art of codifying messages, so that the messages become unreadable, this way it plays a vital role in the field of security of data. There are several Cryptographic Algorithms to encrypt and decrypt Images. This paper aims to Encrypt and Decrypt Images based on RSA Algorithm providing Authentication and using Image Hash functions for additional Security and Integrity of images. This project also makes sure the Image retains its quality and is not corrupted even after decryption.

Keywords : Cryptosystems, Encryption, Decryption, RSA Algorithm, Image Quality Techniques, Authentication

I. INTRODUCTION

RSA Algorithm is most popular and proven asymmetric key cryptographic algorithm. A number various algorithms were proposed for public-key cryptography. Some of these were initially promising but later turned out be breakable.

At MIT, Ron Rivest, Adi Shamir, and Len Adleman created one of the first effective solutions to the problem in 1977. It was initially published in 1978.Since then, the Rivest-Shamir-Adleman (RSA) scheme has dominated as the most extensively used and adopted general-purpose method of public-key encryption.

The plaintext and ciphertext of the RSA cipher are integers with a range of 0 to n-1 for some n. An average size of n is 1024 bits, or 319 decimal places, or n 21024. The RSA algorithm unlike few Symmetric algorithms are not based permutation and combinations, but is rather dependent on mathematics that is to find and multiply large prime numbers with each other. It is based on very large prime numbers. With these large prime numbers one can generate a pair of keys (a Public Key and a Private Key).

So we can say that RSA allows you to be at ease with messages before you send them. And the approach moreover helps you to certify your notes, so recipients will know that their messages are not adjusted or

altered even as in transit. The computers that are made by LG, Toshiba and Samsung are the devices that are embedded with an RSA-Enabled Chip.

Images are widely used over Internet which is a medium of increasing growth of multimedia transfers. So it is very important to secure these images from cryptanalysis and cryptanalysts and ensure that the transfer of these images are complete from one place to another over internet and is not altered or corrupted by hackers.

To secure the Images or Data the first step is Encryption where the data is converted into unreadable or non-understandable form. Later when the transmission of the data is complete it retains back the original form by using the algorithm techniques. This process is Decryption, where the unreadable form is converted back to original data. Additional protection can be provided to this process by providing User Authentication and using Image hash functions.

In case of Image encryption and decryption, we also need to make sure once the Image is retrieved back, the quality of the image is not compromised. There are a few parameters to check the Image Quality, few of these include methods like PSNR, SSIM and MSE. In this project we have used SSIM and MSE to check the image quality.

II. CRYPTOGRAPHY TECHNIQUES OR CRYPTOSYSTEM

To ensure security and integrity of data several cryptographic techniques are used. Basically, there are two Cryptographic systems, depending on the keys used. They are: Symmetric Key Cryptography (same key) and Asymmetric Key Cryptography (different keys).

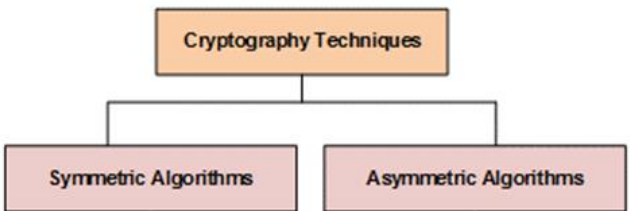


Figure-1. Cryptographic Techniques

A. Components of Cryptosystem

These are the essential components of cryptosystems.

1. **Plaintext:** The algorithm's input for a message or piece of data where the data is in understandable form.
2. **Ciphertext:** This is the encrypted message produced as an output which is in unreadable format. It depends on the key and the plaintext.
3. **Encryption Algorithm:** The encryption algorithm changes the plaintext (readable communication) in a myriad of areas and outputs ciphertext as a result.
4. **Decryption Algorithm:** It produces the plaintext as an output which takes the secret key and the ciphertext as inputs. It generally performs the reverse process of Encryption.
5. **Public and Private key:** Asymmetric and Symmetric Cryptosystems both use public key (knowing to all) and private key (known just to the user) and these are the pair of keys where one key is used for encryption and the other for decryption.

B. Types of Cryptosystems

Symmetric Key Cryptosystem

It is a process that uses only one key that is secret key to decrypt and encrypt a message to protect it from cryptanalysts.

Ex: DES, AES and 3-DES.

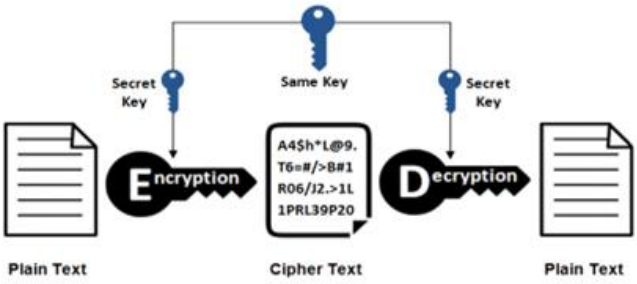


Figure-2. Symmetric Key Cryptosystem

Asymmetric Key Cryptosystem

Another name for this system is Public Key Cryptosystem. Here, the encryption and decryption keys used by the sender and receiver are distinct.

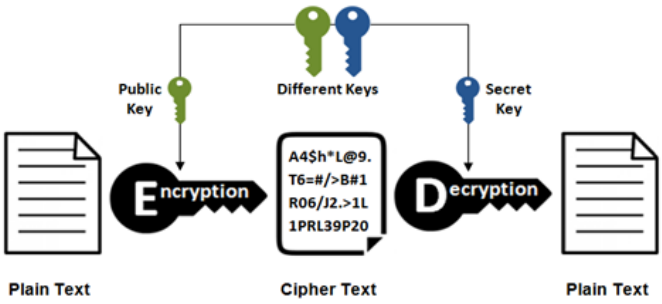


Figure-3. Asymmetric Key Cryptosystem

Ex: Diffie-Hellman, RSA, DSA and ECC

III. OBJECTIVES

The main Objectives of this project:

- Simulation of RSA algorithm to ascertain encryption and decryption.
- To develop an optimized algorithm using the 2 prime numbers to generate encryption and decryption keys to enhance data security goals such as confidentiality, authenticity, secrecy and integrity.
- Comparison of the approach/results with existing ones.
- Compares the quality of original image with the Decrypted image

IV. METHOD OF IMPLEMENTATION

Input Image: The image which has to be encrypted.
Key Generation: It is the first step in RSA algorithm. The generation of a pair of keys is necessary before using the public key cryptosystem. These tasks are included in this:

1. To determine 2 prime numbers, p and q.
2. Select either d or e and then calculate the other.

A. RSA Algorithm

Exponential Expressions are used by RSA. Typically, plaintext is encrypted in blocks, with each block having a binary value < n, or a block size ≤ $\log_2(n) + 1$; $2^i < n \leq 2^{i+1}$, where i is the block size in bits. The RSA-768 Challenge, which has a key length of 768 bits or 232 in decimal digits, is the most recent challenge to be overcome in the attack on RSA. Therefore, 1024 to 2048 key bits or more should be considered appropriate. The sender and the recipient are both aware of the value of n. Only the receiver is aware of the d value; the sender is aware of the e value.

Working of RSA Algorithm

- Consider 2 huge prime numbers from image pixels p, q such that p ≠q.
- Calculate n= p x q, $\phi(n) = (p-1)(q-1)$
- Select e such that $\gcd(e,\phi(n)) \equiv 1$.
- Calculate d using Extended Euclidean algorithm ($d \equiv e^{-1} \bmod \phi(n)$)
- Public key = {e, n}
- Private key = {d, n}
- Encryption
  $C = M^e \bmod (n)$ where C = Ciphertext and M = Plaintext.
- Decryption
  $M = C^d \bmod (n)$

B. Authentication:

It recognises user's identity and it confirms who they say they are. Usually in authentication process the computer or the user needs to prove their identity to the clients or servers which involves username and password or other methods like fingerprint, facial scan, voice biometrics and captcha text.

C. Image Hash Functions:

It is a process of assigning a unique hash value to the image with the help of an algorithm. To verify the accuracy of the photos, Image Hash is used in place of cryptographic hash methods like SHA-256 and MD5 Algorithms.

D. Autocorrelation:

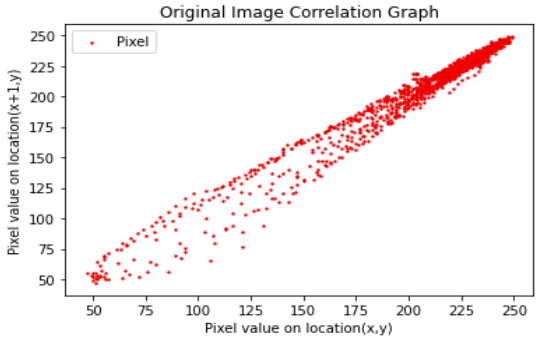
The autocorrelation function is used to find patterns in data. Every original image will have certain patterns in the autocorrelation plot. For good algorithm the encryption correlation plot should appear random with no identifiable patterns. This reduces the statistical analysis attacks on the cipher image.

The pixels are selected randomly in horizontal, diagonal and vertical directions in both the plain and encrypted images and calculate the correlation degree

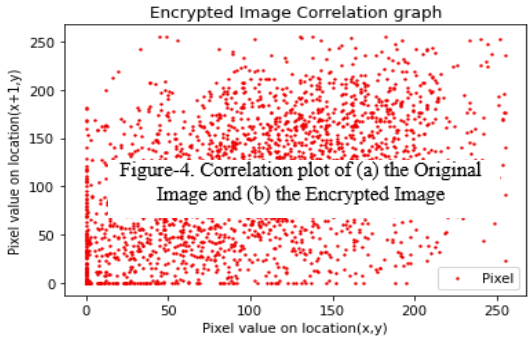
$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2}},$$

with the expression,

where x and y are neighbouring pixels in different directions and $E(x) = \frac{1}{N}\Sigma_{i=1}^{N} x_i$.



(a)



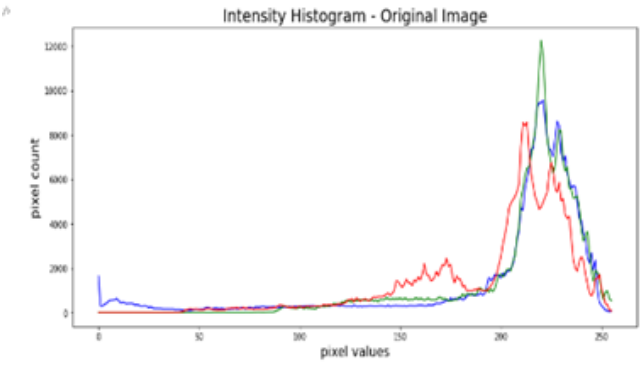
(b)

Figure-4. Correlation plot of (a) the Original Image and (b) the Encrypted Image

V. IMAGE QUALITY TECHNIQUES

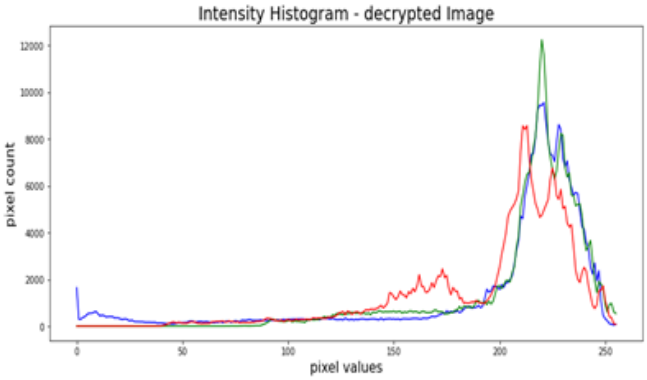
A. Histogram Analysis

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.



(a)

(b)



(c)

Figure-5. Histogram plot of (a) Original Image, (b) Encrypted Image and (c) Decrypted Image.

B. Structural Similarity Index Measure (SSIM)

It is used for measuring the similarities between two images. The initial distortion or Uncompressed of free image predicts the Image Quality. Generally, the value

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x + \sigma_y + c_2)}$$

varies between 0-1. 1 implies perfect match with the original image.

C. Mean Squared Error (MSE)

The statistical models like images and data uses MSE to measure the amount of error in it. It is the sum of squared difference between the two images. The two images must have the same dimensions. The MSE equals zero when the model has no error.

$$MSE = \frac{1}{n}\frac{1}{m}\sum_{i=1}^{n}\sum_{j=1}^{m}(Y(i,j) - \hat{Y}(i,j))^2$$

VI. RESULTS

Here it is shown that Images of almost all sizes can be encrypted and decrypted. The results are as shown below.

(a)

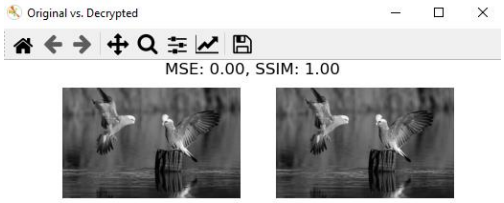
(b)

(c)

Figure-6. (a)Original Image, (b) The Encrypted Image and (c) The Decrypted Image

The SSIM and MSE values for the respective images are as shown below.

(a)



(b)

Figure-7. (a) SSIM and MSE values of Original Image Vs Encrypted Image (b) Original Image Vs Decrypted Image.

VII. DISCUSSIONS

Simulation of RSA algorithm on images and respective Encrypted and Decrypted Images are being displayed.

Authentication is provided for the Encryption and Decryption process with their respective user credentials for additional protection of the data.

The Scattered Pattern of Autocorrelation graph shows that the Algorithm is a good algorithm for Encryption of Images.

Comparison of the approach/results with the existing ones.

Compares the quality of the Original Image with the Decrypted Image.

VIII. CONCLUSION

In our project we have shown the implementation of the RSA Algorithm obtaining the final results in the form of Image Encryption and Decryption. This project is also provided with Authentication and Image Hash functions for integrity. We have also used SSIM and MSE for Image Quality evaluation.

IX. FUTURESCOPE

- Further other algorithms can be used together and compared.
- Encryption for Audio or video can also be implemented further.
- Steganography can also be used to enhance encryption.

III. REFERENCES

[1]. Nadjia Anane, Mohamed Anane2, Hamid Bessalah, Mohamed Issad1, Khadidja Messaoudi1, et.al [1], presents "RSA Based Encryption Decryption of Medical Images".

[2]. Aman Jain, Simran Sharma, et.al [2] describes "Digital Image Encryption using RSA algorithm.

[3]. 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 .

[4]. 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.

[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]. J. Sahu, V. Singh, V. Sahu, and A. Chopra, "An enhanced version of RSA to increase the security," J. Netw. Commun. Emerg. Technol., vol. 7, no. 4, pp. 1–4, 2017.

[8]. P. Gupta, D. K. Verma, and A. K. Singh, "Improving RSA algorithm using multi-threading model for outsourced data security in cloud storage," in Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence), Jan. 2018, pp. 14–15.

[9]. I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," Telkomnika (Telecommun. Comput. Electron. Control., vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13201.

[10]. 10.Raza Imam 1 , Qazi Mohammad Areeb 1, Abdulrahman Alturki 2 , And Faisal Anwer 1, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status",10.1109/Access.2021.3129224.

[11]. Nevart A. Minas1, Faten H. Mohammed Sediq, Adnan Ibrahem Salih,"Color Image Encryption Using Hybrid Method of Fractal- Based Keyand Private XOR Key", Kirkuk University Journal /Scientific Studies(KUJSS), vol. 13, no. 1, October 2018.

[12]. C. A. Sari, G. Ardiansyah, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," Telkomnika, vol. 17, no. 5, pp. 2400–2409, 2019.

[13]. C. Vyas and J. Dangra, "A review of modern cryptography techniques with special emphasis on RSA," Int. J. Technol. Res. Manage., vol. 4, pp. 2348–9006, Jul. 2017, Accessed: Aug. 12, 2021.

[14]. S. Saxena and B. Kapoor, "State of the art parallel approaches for RSA public key based cryptosystem," Int. J. Comput. Sci. Appl., vol. 5, no. 1, pp. 81–88, Feb. 2015, doi: 10.5121/ijcsa.2015.5108.

[15]. P.O.Asagba and E. O. Nwachukwu, "A review of RSA cryptosystems and cryptographic protocols," West Afr. J. Ind. Academic Res., vol. 10, no. 1, pp. 3–16, 2014.

Cite this article as :

Radhakrishna M, Shridevi K S, Sowmya B S, Sushmitha T J, "Digital Image Encryption and Decryption based on RSA Algorithm", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 4, pp. 168-173, July-August 2022. Available at doi :

https://doi.org/10.32628/IJSRSET229431

Journal URL : https://ijsrset.com/IJSRSET229431