Image Encryption/Decryption Using AES & RSA Algorithms

Prof. Shailendra Gaur[1*] **, Ariba Saher**[2]

[*1] Assistant Professor, Department of Information Technology, BPIT, Delhi, India

[2] Department of Information Technology, BPIT, Delhi, India

Abstract: In recent years information security has become a vital issue. Transmitting data over the non-secured media allowed the unauthorized users to access and manipulate the information. To beat this, the information is being sent or kept in an encrypted format. Cryptography is an art or science of writing secret codes. It involves changing of data/file from human legible form to non-human legible form and then converting it back to its original form. There are three kind of cryptography techniques: symmetric key cryptography, asymmetric key cryptography and hash function. Symmetric key cryptography algorithms include: DES, Triple-DES(3-DES), Blow fish etc. And asymmetric key cryptography algorithms include: RSA, ECC etc. This project is aimed towards making use of AES and RSA algorithms for Encryption/Decryption of the images. Encrypted Image developed using these algorithms will be completely different when compared to the initial image. This project also aims towards the secure transmission of encrypted images over the internet.

Keywords: Encryption, Cryptography, Symmetric key cryptography, asymmetric key cryptography, AES, RSA.

1. Introduction

Image security is an utmost concern within the internet. The Image encryption and decryption has various applications like communication over the internet, imaging in medical, communication in military or government etc. To make the data secure from web attacks it must be encrypted or must be kept in encrypted form. The state, institutes, hospitals and army deals with images about their plans, strategies, patients and enemies on a daily basis and as everyone nowadays store this confidential information on their devices and transmits over the web. If this information gets in the hand of someone unauthorize it may have some serious consequences and may cause damage beyond repair.

Cryptography is used to encode the data stored on devices or transmitted over some channel to ensure that no unintended user can access it. Moreover, cryptography is utilized to secure the method of confirming distinctive parties endeavoring any work on the framework. Since a party wishing be allowed a certain usefulness on the framework must show something that demonstrates that they infact who they say they are. That something is now and known as accreditations and extra measures must be taken to guarantee that these accreditations are as it were utilized by their legitimate party. The foremost classic and self-evident credential are passwords. Passwords are scrambled to ensure against illicit utilization. Security of web keeping money account passwords, mail accounts etc. requires content assurance in advance media.

Dissimilar to instant messages, the interactive media data including picture information has some unique attributes like excess and high relationship among pixels. One of the primary objectives that must be accomplished during the transmission of data over the system is security. This method will cause the data to be transmitted into an incomprehensible structure by encryption with the goal that solitary approved people to can effectively recoup the data. Encryption is the way toward changing a snippet of data, known as the plaintext, utilizing an algorithm, to make it unreadable to anybody with the exception of those having uncommon information, for the most part alluded to as a key. The final outcome is known as the ciphertext. Reversing the ciphertext back to the original form is known as decryption.

2. Types of Cryptography

There are three types of cryptography techniques [1]:

1. Symmetric key Cryptography

2. Asymmetric key Cryptography

3. Hash Functions

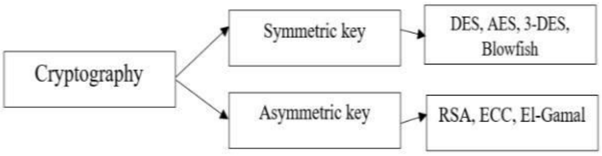


Fig.1 Types of Cryptography

2.1 Symmetric key Cryptography: In this strategy just one key is utilized for both encryption and decoding process and the key are traded between the sender and the beneficiary over some verified transmission medium. Algorithms: DES, AES, 3-DES, Blowfish and so on.

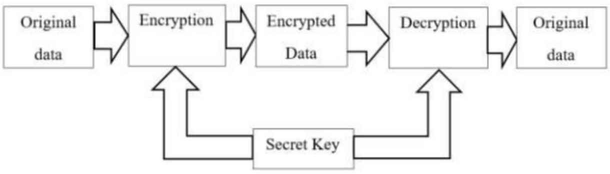


Fig. 2 Symmetric Key Cryptography

2.2 Asymmetric Key Cryptography: In this strategy open key is utilized for encryption and private is utilized for decoding process and the private key is traded between the sender and the recipient over some verified transmission medium. Algorithms: RSA, ECC etc.

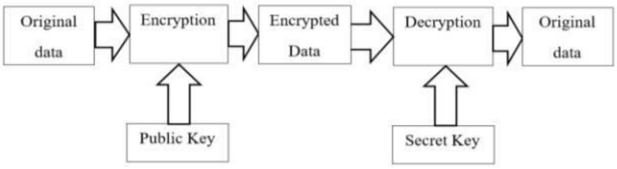


Fig. 3 Asymmetric Key Cryptography

3. Related Work

Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, et. al. [2] clarified about a picture cryptography it might utilize the conventional cryptosystems to scramble pictures. In any case, it having two issues. The principal issue is that the picture size is in every case a lot more noteworthy than content. Along these lines, the cryptosystems are need a lot of time to encode the picture. The subsequent issue is the decoded information ought to be equivalent to the first information. Because of the Characteristic of human discernment, a decoded picture containing little bending is typically satisfactory.

Ambika Oad, Himanshu Yadav, Anurag Jain, et. al. [3] prescribed the picture encryption is a strategy which is convert the first picture into another configuration that is hard to comprehend. Along these lines, without realizing the unscrambling key nobody can get to the data. The picture encryption has applications in corporate world, human services, military tasks, and media frameworks. Encryption is the procedure which is encoding the plain content into figure content, and the invert procedure of changing over figure content into the plain content is decoding. The cryptography comprises of encryption and unscrambling strategies.

Komal D Patel, Sonal Belani, et. al [4] proposed the picture encryption methods are convert the first picture to another picture that is difficult to comprehend, it is keep the picture private between clients. It is fundamental that no one can't to get the data without a key for decoding. Besides, extraordinary and dependable security in transmission the advanced pictures is required in numerous applications, for example, military picture interchanges, digital TV, online individual photo collection, restorative imaging frameworks and secret video meetings, and so on. So as to satisfy such an undertaking, and have been proposed many picture encryption techniques.

4. Encryption Algorithms

4.1 AES Algorithm

The AES [5] algorithm is of three types i.e. AES-128, AES-192 and AES-256. This order is done on the bases of the key utilized in the algorithm for encryption and unscrambling process. The numbers speak to the size of key in bits. This key size decides the security level as the size of key expands the degree of security increments. The AES calculation utilizes a round capacity that is made out of four diverse byte-arranged changes. For encryption reason four rounds comprise of:

- Substitute byte
- Shift row
- Mix columns
- Add round key

While the decoding procedure is the turnaround procedure of the encryption which comprises of:

- Inverse shift row
- Inverse substitute byte
- Add round key
- Inverse mix columns

There is various round present of key and block in the algorithm. The quantity of rounds relies upon the length of key use for Encryption and Decryption.

4.2 RSA Algorithm

The RSA [6] algorithm is fundamentally implied for content encryption. As there is a noteworthy requirement for giving security on picture transmission, this paper is stretching out the RSA algorithm to perform picture encryption and decoding. At first, two prime whole numbers p and q are taken which are utilized for ascertaining keys (private key and open key) and choosing the info picture for encoding. „e‟ and d are chosen so that =1. The chose picture is encoded by utilizing the equation. P is the information picture we are encoding. „e‟ is the general population key which is utilized for scrambling. Φ(n) is the result of (p-1) and (q-1) with the end goal that gcd(e,φ(n)) =1 for example e and Φ(n) are coprime. C is the figure picture created after encryption is finished. We are unscrambling the scrambled picture utilizing the recipe C is the figure picture after it has been encoded. „d‟ is the private key which is utilized to unscramble the figure picture. „n‟ is the result of (p-1) and (q-1) with the end goal that, this is all the more obviously expressed as:

Algorithm for Encryption and Decryption

1. Read the input RGB color image, S

2. First choose the two distinct prime numbers p and q.

3. Calculate the value, n = pq.

4. Compute φ(n) = φ(p)φ(q) = (p − 1) (q − 1) = n - (p + q -1), where φ is Euler's totient function.

5.Choose an integer e such that 1 < e < φ(n) and gcd (e, φ(n)) = 1; i.e., e and φ(n) are co-prime. e is the released as the public key.

6.Determine d as d ≡ e −1 (mod φ(n)); i.e., d is the modular multiplicative inverse of e (modulo φ(n)). Solve the d given d·e ≡ 1 (mod φ(n)).

7. Obtain the encrypted image, C = Se mod φ(n).

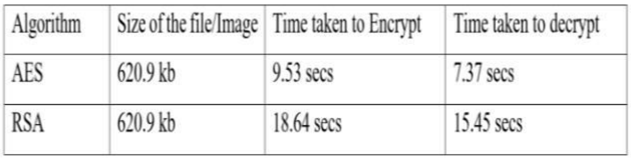
8. C = C mod 256, as gray level values of an image lie in the range [0,255].

9. Recover decrypted image, S = Cd mod 256.

10.The original input (recovered) image, R = S mod φ(n).

5. Results

Experimental results for Encryption algorithm AES and RSA are shown below:



Algorithm	Size of the file/Image	Time taken to Encrypt	Time taken to decrypt
AES	620.9 kb	9.53 secs	7.37 secs
RSA	620.9 kb	18.64 secs	15.45 secs

Table.1 Experimental result for Encryption algorithm AES and RSA Algorithms

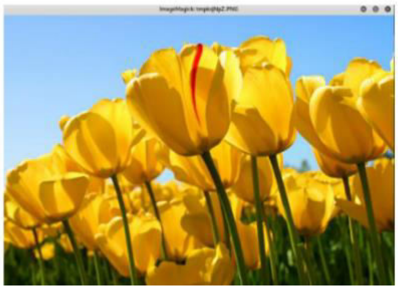


Figure.4 Original Image

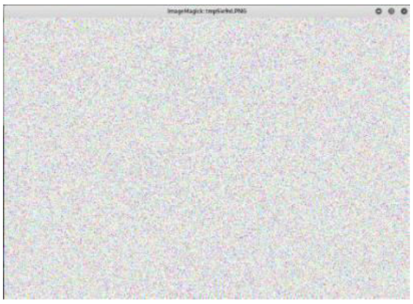


Figure.5 Encrypted image developed Using AES algorithm

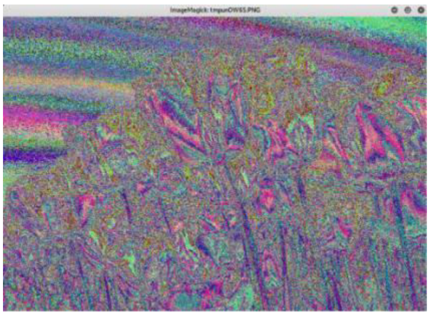
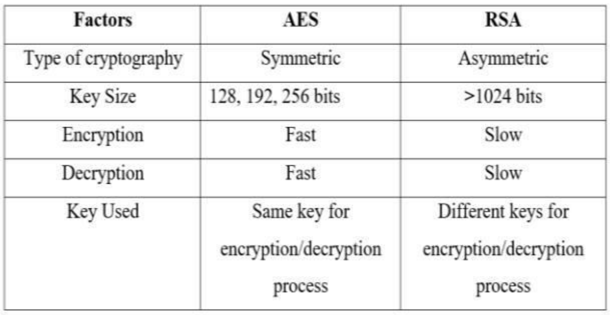


Figure.6 Encrypted image developed using RSA algorithm

6. Comparison

E. Thambiraja, G. Ramesh, Dr. R. Umarani [7] have done survey on most common encryption techniques. Monika Agrawal and Pradeep Mishra [8] in have also done a comparative survey on Secret Key Encryption Techniques. Gurujeevan Singh, Ashwani Kumar Singla, K.S.Sandha [9] in have provided comparison of various cryptography technique algorithms.

In the table given below, comparison between AES & RSA algorithms is shown:



Factors	AES	RSA
Type of cryptography	Symmetric	Asymmetric
Key Size	128, 192, 256 bits	>1024 bits
Encryption	Fast	Slow
Decryption	Fast	Slow
Key Used	Same key for encryption/decryption process	Different keys for encryption/decryption process

Table.2 Comparison between AES & RSA algorithm

7. Conclusion

In this paper, two algorithms to be specific AES & RSA have been summarized. From the results and analysis mentioned above, we can say that both the Algorithms have their own merits and demerits. As AES is a secret key based algorithm which suffers from key distribution, but the Encryption/decryption process is fast. While the RSA is an open key-based algorithm in which the key dispersion issue has been survived yet the encryption/decoding process takes additional time when contrasted with AES.

REFERENCES

[1] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008

[2] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), ISSN 2249-6343 International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.

[3] Ambika Oad, Himanshu Yadav, Anurag Jain, A Review: Image Encryption Techniques and its Terminologies, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[4] Komal D Patel , Sonal Belani, Image Encryption Using Different Techniques: A Review International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011.

[5] Daemen.J and Rijmen, The Advanced Encryption Standard, Dr. Dobb's Journal, March 2001

[6] Rivest R, Shamir A, Adleman L, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of ACM 21 (2): 120–126. doi:10.1145/359340.359342 (February 1978).

[7] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[8] Monika Agrawal, Pradeep Mishra", A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol.4 May 2012.

[9] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 201