Digital Data Encryption and Decryption using RSA and AES Algorithms

Conjeevaram Sankeerthana, Medipally Jhansi, Mrs.Shilpa B. Darvesh

Department of Electronics and Communications, Maturi Venkata Subba Rao Engineering College, Hyderabad, India

Assistant Professor, Department of Electronics and Communications, Maturi Venkata Subba Rao Engineering College, Hyderabad, India

Abstract— **These days, there are a lot of online frauds or cybercrimes that take place at almost every country in the world. In such types of incidents, the sensitive or confidential data such as text messages, images, passwords, or usernames are hacked or known by a third person apart from the owner of the data. To avoid such blunders, a technique known as cryptography is bought into action. Cryptography is a technique which primarily consists of two main processes known as encryption and decryption. Encryption is a process of converting the input data into an unreadable form which is completely different from the input data to protect it from getting into unsafe hands. Similarly, decryption is the process for converting the encrypted data into a readable form or back to its original form where only the intended recipient can receive the decrypted data. Cryptography gets its name from the combination of two Greek words, "crypto" which means secret and "graphy" which means writing which together means hidden or secret data or information. Cryptography allows secure and safe transmission of data from a sender to the intended recipient. Cryptographic algorithms can be widely classified into three types such as Asymmetric Key Algorithms, Symmetric Key Algorithms and Hash Functions. In this paper, we are executing digital data or image cryptography or encryption and decryption using RSA, Rivest-Shamir-Adleman algorithm and AES, Advanced Encryption Standard algorithm through MATLAB Software. Image encryption can be termed as the process of encoding or ciphering a secret image using an encryption algorithm such that the image does not get into the hands of unauthorized users other than the receiver. Similarly, image decryption can also be termed as the process of converting the encrypted image or the ciphered image back to its original form. By using a combination of both RSA and AES algorithms for image cryptography, we can eliminate the existing disadvantages of individual algorithms like complexity, speed, key size, and management of data in RSA algorithm and key authentication and integrity in AES algorithm. Values like Mean Square Error (MSE), Peak Signal to Noise ratio (PSNR) are calculated for combined RSA and AES algorithm procedure. The image factors like Accuracy, Sensitivity and Specificity are obtained and compared for RSA and AES algorithms individually and combined as well.**

Index Terms- **Cryptography, RSA algorithm, AES algorithm, Discrete wavelet Transformation, Accuracy, Sensitivity, Specificity.**

I. INTRODUCTION

Image data security is one of the most important requirements for communication processes and multimedia procedures. The access to sensitive data or secured data of a person other than the sender or the intended receiver or the owner of the data while sharing or storing data is mostly dangerous. The information can get into hands of scammers or fraudsters who can use our data for monetary purposes or imposing or for terrorist crimes. Cryptography is one among the better techniques for image or digital data security which involves use of protective algorithms like RSA algorithm and AES algorithm. There are many other algorithms also like DES apart from RSA and AES algorithms. RSA algorithm is a form of an asymmetric key algorithm which uses two different and unidentical or asymmetric keys; one is a public key which can be accessed by anyone which is used for encryption process and the other is a private key which is not accessible to public but only accessible to the recipient intended and used during the decryption process. This algorithm was introduced by three MIT colleagues named, R. Rivest, A. Shamir and L. Adleman in the year 1997. AES is a symmetric key algorithm unlike RSA which uses a single key or a shared key accessible to both the sender and the recipient. The same key is used for both the encryption and the decryption processes. It is also known as Rijndael algorithm as it was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen in the year 2001.

EXISTING METHOD: There are various other methods of Image cryptography. [1] One such method includes FPGA (Field Programmable Gate Array) implementation of RSA algorithm which is not feasible for many as it becomes an expensive process due to the necessity of an FPGA board (SPARTAN board). To ensure efficiency of the encryption process of shared key by the RSA algorithm, they made use of histograms of key images before and after the encryption process which were generated and analysed for their encryption strengths. There are many other methods with algorithms like RSA, AES, DES, individually or by using Differential expansion technique.

In this paper, we primarily aim to perform the cryptography or the process of encryption and decryption of an image which is a also a form of digital data using a combination of both the required algorithms which include a Symmetric key algorithm, AES and an asymmetric key algorithm, RSA. The Discrete wavelet Transformation (DWT) technique is used for combining both the algorithms to obtain the desired result. The comparison between the algorithms individually and combined is obtained using parameters like Accuracy, Sensitivity and Specificity.

II. OPERATION OF THE PROPOSED MODEL

Since digital data such as images can be easily manipulated or copied, cryptography is a technique used to secure the data for various applications like multimedia security, banking, financial privacy etc. The symmetric key algorithm, AES requires both sender and the receiver to use a single shared key. But this may create a problem if the shared key is not secure enough. Whereas the asymmetric key algorithm, RSA uses two different keys but it may not be a feasible option if data is large. Thus, in our proposed method, a combination of both the algorithms is used to obtain better output.

Figure 1 shows the algorithm or flowchart with all the steps involved of the process. The major steps involved in the process are Image Acquisition, Pre-processing, Transformation, Embedding, Encryption, Inverse transformation, and Decryption. Finally, the comparison of factors of the algorithms like Accuracy, sensitivity and Specificity is carried out for obtaining the result.

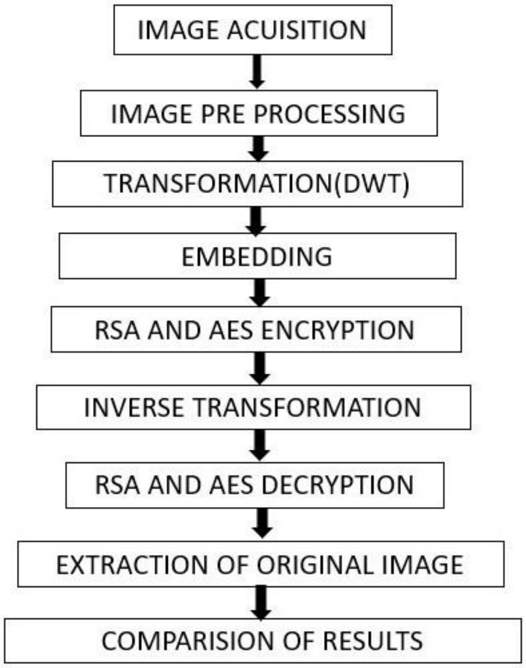


Figure 1: Block diagram representing the process of image encryption and decryption using RSA and AES algorithms

II.A Image Acquisition

Image acquisition is the process to acquire a digital image. It requires an image sensor and capability to digitize signal produced by the sensor. The image sensor could be a line scan camera that produces a single image line at a time and the motion of the object past the line. If the output of the camera or the imaging sensor is not in a digital form, then an analog to digital converter (ADC) is used to digitize the image.

II.B Image Pre-Processing

Image Pre-processing is used for operating the image at its lowest level of abstraction. At this level, both the input and output are considered as intensity images. It provides an improvement of the image by supressing the unwanted distortions and enhances the features of the image for further processing according to requirements necessary.

II.C Transformation

Transformation technique is done to modify or transform the image as per our requirement. In this proposed paper, we are using Discrete wavelet transformation (DWT) technique. This is used mainly in image processing where the wavelets are discretely sampled. We are using four filter combinations which are:

1. Low pass filter – Low pass filter
2. Low pass filter – High pass filter
3. High pass filter – Low pass filter
4. High pass filter – High pass filter

II.D Embedding

Embedding is one of the most crucial steps of the process and is executed after the DWT transformation. In embedding, both the text (secret data or secret key) and the transformation image (from DWT) are combined for further processing at the image encryption stage.

II.E RSA and AES algorithms encryption and decryption

RSA Encryption and Decryption:

RSA is an asymmetric key algorithm which makes use of two different keys known as public key and private key for encryption and decryption processes respectively.

To find the keys, first let us select two random large prime numbers which are p and q.

An integer n is found which is the product of these 2 numbers;

$$n = p*q$$

Let us assume another number f such that;

$$f = (p-1) * (q-1)$$

We must select an integer e such that $0 < e < 1$ or e lies between 0 and 1.

The encryption key or public key is given by (e, n)

Plain text (message) = M

Cipher text (encrypted message) = C

$$C = M ^\wedge (e \bmod n) \text{ where } M < n$$

Decrypted key, d is chosen such that $d ^\wedge (e \bmod f(n)) = 1$

The decrypted message (original message) is obtained by:

$$M = C ^\wedge (d \bmod n)$$

This is about encryption and decryption process in RSA algorithm.

AES Encryption and Decryption:

AES is a symmetric key algorithm which uses a single shared key or a same key for both encryption and decryption processes.

The fixed block length of the algorithm can be taken as 128 bits.

The length of the key size can be anything such as 128 bits ,192 bits or even 256 bits.

For encryption, AES requires a separate 128-bit round key block for each round including one more. The following processes take place:

1. Initial round (Add round key, each byte of state is combined with a block of round key using Bitwise XOR.)
2. Iterative round (Sub bytes, Shift rows, mix columns, add round keys.)
3. Final round (Sub bytes, shift rows, add round key.)

Decryption is the inverse process of encryption. In this, inverse sub bytes, inverse shift rows, inverse mix columns are used in reverse order instead of sub bytes, shift rows and mix columns. The key expansion is maintained as same.

II.F Inverse transformation

As in the above process we have seen that DWT or Discrete wavelet transformation takes place, similarly, an Inverse transformation technique is also executed to obtain the result in its original form rather than the transformed form.

II.G Creating GUI (Graphic User Interface)

A graphical user interface (GUI) is a graphical display software which is used for windows which is used for controlling the desired components. It also allows the users to perform many other interactive tasks. We are using the GUI interface for creating the various MATLAB tools required for successfully implementing the project. It can be used to read or write the data files or for graphical description of the result plots or for interacting with some other GUI's.

II.H Factors

The various factors that are calculated and observed in this paper are as follows:

1. Mean Square Error (MSE):

MSE = sum (sum (squared Error Image)) / (rows *columns)

2. Root Mean Square Error (RMSE):
   RMSE = sqrt (MSE)
3. Peak Signal to Noise Ratio (PSNR):
   PSNR = 10 * log10 (256^2 / MSE)

The image factors such as Accuracy, sensitivity and specificity are measured using the following terms:

Tp (true positive) = Abnormality correctly classified as abnormal.

Tn (true negative) = Normal correctly classified as normal.

Fp (false positive) = Normal incorrectly classified as normal.

Fn (false negative) = Abnormality incorrectly classified as abnormal.

4. Accuracy = ((Tp+Tn)/(Tp+Tn+Fp+Fn)) *100
5. Sensitivity = (Tp/(Tp+Fn)) *100
6. Specificity = (Tn/(Tn+Fp)) *100

III. SIMULATION RESULTS

1.Input Image and DWT Image

In the Figure 2, we can see two images. The first figure shows the input image which has been selected for encryption but in grey form (black and white) while the second image is the DWT (Discrete Wavelet Transform) image of the input image. The DWT image has been divided into four segments based on the four filter combinations mentioned above.

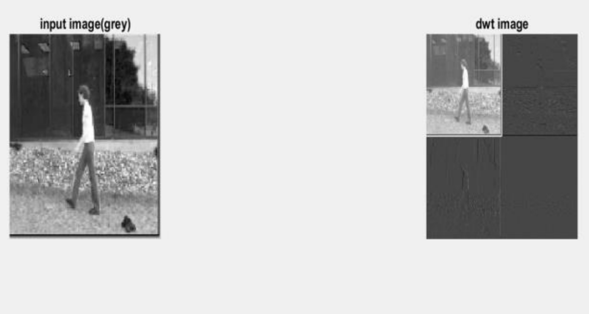


Figure 2

2. Encryption Images

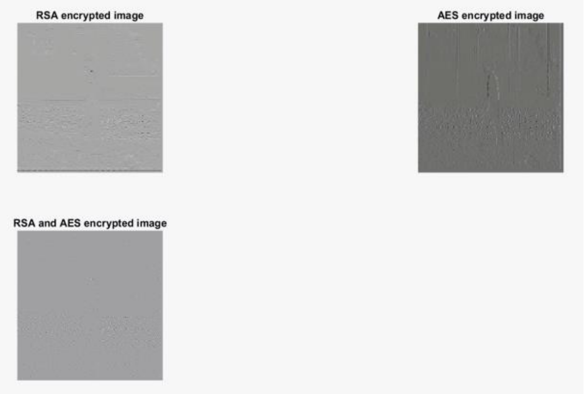


Figure 3

Figure 3 represents the encrypted images using RSA and AES algorithms, individually as well as in combined form. From the figure, we can see that the AES encrypted image has the least level of encryption i.e., the input image is comparatively clear. It is also noticed that RSA and AES (combined) encrypted image is much more secure in terms of encryption as the input image is not at all visible.

3. Decryption Images

Figure 4 represents the decrypted images of RSA algorithm and AES algorithm individually and RSA and AES algorithms combined.

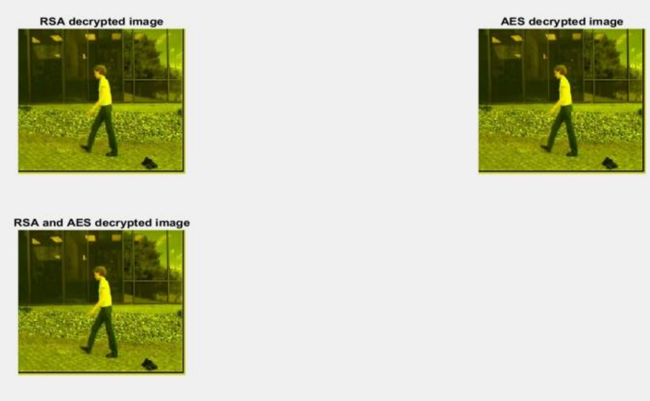


Figure 4

4. RSA and AES decrypted image parameters

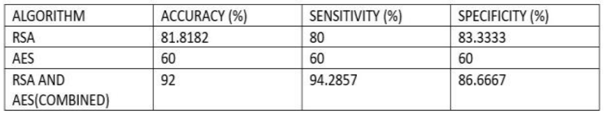
The Mean Square Error, Root Mean Square Error and Peak Signal to Noise Ratio factors are calculated for the proposed method (RSA and AES algorithms combined). They are:

MSE = 231.614588

RMSE = 15.218889

PSNR = 21.483145

5. Comparison Results



ALGORITHM	ACCURACY (%)	SENSITIVITY (%)	SPECIFICITY (%)
RSA	81.8182	80	83.3333
AES	60	60	60
RSA AND AES(COMBINED)	92	94.2857	86.6667

Figure 5

Figure 5 is the table comparing the values of Accuracy, Specificity and Sensitivity for RSA algorithm, AES algorithm and RSA and AES algorithm combined. From the table we can see that RSA and AES combined algorithm produces an efficient output.

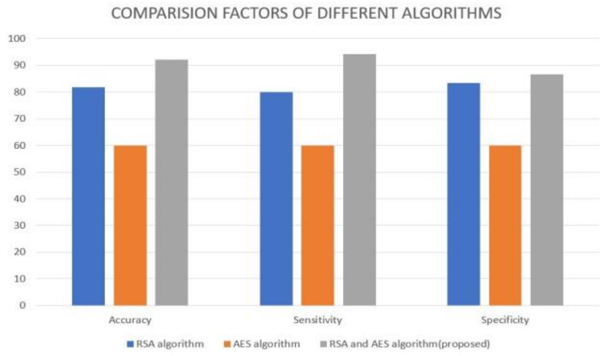


Figure 6

Figure 6 is the graphical illustration of the above table represented in Figure 5. The graph compares the factors Accuracy, Sensitivity and Specificity of the three algorithm techniques in different colors. The RSA and AES combined cryptography technique has better outcome in all the three factors Accuracy, Specificity and Sensitivity.

IV CONCLUSION AND FUTURE SCOPE

This paper emphasizes on the technique of combined use of RSA and AES algorithms for image cryptography to obtain better output results. By combining both the algorithms, the individual drawbacks of both the algorithms are reduced and the overall efficiency of the crypto system is increased. From the results, we can see that the RSA and AES combined algorithm has higher Accuracy, Specificity, and Sensitivity.

The proposed paper can be improvised in the future by combining it another algorithm or using a combination set of some other algorithms for a better result.

This technique of cryptography can be used not only for digital data (image) but also for videos or chain of images etc.

REFERENCES

1. An FPGA implementation of the RSA algorithm using VHDL and a Xilinx system generator for image applications, which is written by Sandeep Saini, Kusum Lata, Abhishek Sharma and G R Sinha, IOP Publishing Ltd (2021).
2. “A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB”, written by authors Karrar Dheiaa Mohammed Al-Sabti and Hayder Raheem Hashim, Global Journal of Pure and Applied Mathematics. ISSN 0973-1768 Volume 12, Number 4 (2016).
3. “Performance Analysis of Encryption Algorithms for Security,” with author Madhumita Panda, International conference on Signal Processing, Communication, Power, and Embedded System (SCOPES)-2016, IEEE.
4. “Comparative Study of AES, RSA, Genetic, Affine Transform with XOR Operation, And Watermarking for Image Encryption” written by the authors Avinash Ray, Anjali Potnis, Prashant Dwivedy, Shahbaz Soofi, Uday Bhade, Proceeding International conference on Recent Innovations is Signal Processing and Embedded Systems (RISE-2017) 27-29 October,2017.
5. Idrizi, Florim, Dalipi, Fisnik and Rustemi, Ejup. “Analyzing the speed of combined cryptographic algorithms with secret and public key”. International Journal of Engineering Research and Development, e-ISSN: 2278- 067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (2013), pp. 45
6. Abdul. Mina, D.S, Kader, H.M. Abdual and Hadhoud, M.M. “Performance Analysis of Symmetric Cryptography.” pp. 1.
7. Chehal Ritika, Singh Kuldeep. “Efficiency and Security of Data with Symmetric Encryption Algorithms.” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 8, August 2012, pp. 1.
8. Internet, Wikipedia.