Efficient and Secure Transmission of Data

Shweta Manjunath [1], Shwetha C [1], Thayi Deekshitha [1], Vishakha Shubham [1], Pushpa B. R. [2]
[1]Student, [2]Assistant Professor
Department of Telecommunication Engineering,
Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India.

Abstract*:* Efficiency in the field of communication is of utmost importance. The efficiency in data transfer is obtained by encrypting the data primarily for security by using the Rivest Shamir Adleman (RSA) encryption algorithm. The RSA encryption provides the data with security by utilizing separate keys for the process of encryption and decryption. Post encryption, the result is encoded using the Reed Solomon (RS) encoding scheme. The added advantage of this encoding scheme is its error detection and correction scheme in addition to the productive bandwidth usage. The data is encoded from the source and will be modulated using Quadrature Amplitude Modulation (QAM) scheme. The modulated data can then be transmitted. The use of modulation improves the reception quality and ensures no signal mixing occurs. In the receiving end, the received signal is demodulated, decoded. The errors are detected and corrected in case if present. In this paper errors are introduced by the user to demonstrate the error detecting and correcting capabilities. The decoded data is then decrypted to obtain the original data. The entire set up is simulated on the MATLAB software.

Index Terms - RSA algorithm, Encryption, Encoding, RS Code, Modulation, Data

I. Introduction

An image is a picture which can be represented in electronic form. It can either be stored in razor or vector form. When stored in vector form it is called a bitmap image. An image can be either two-dimensional or three-dimensional. A grey scale image with the pixel value ranging from 0 to 255 is the input considered.

Rivest Shamir Adleman (RSA) cryptosystem is an algorithm which is used to provide the encryption. This algorithm is used most commonly in encryption and authentication. This algorithm will be used for encryption and decryption process. RSA algorithm is a public key cryptosystem which is very secure as compared to other cryptosystems since there are two keys involved. On the sender's end, we have the public key which is available to everyone and on the receivers end, we have the private key. The private key is not available to everyone but only to a few authentic third parties who have permission to access the information [1]. The usual problems which we face during any image cryptography is that image size is always much greater than the text and another problem faced is that decrypted data should be equal to the original data [2].

Encoding refers to converting one form of data into another. Encoding can be implemented on images, audios, and videos. Reed Solomon encoding and decoding technique is implemented here. Since there is a large variety in which RS codes can be implemented, a comprehensive study and comparison of all the variants of the technique are done [3]. RS (512,201) has been chosen. Reed Solomon decoding procedures help in detecting errors and correct erasures and errors [4]. Also fading factor can cause burst errors in the signal that is being sent through the wireless channel. To rectify the burst errors in the signal Reed Solomon codes were found to be more effective [5].

Modulation is the process in which we change the characteristics of the wave to be transmitted by superimposing the message signal on a high-frequency signal called a carrier signal. Quadrature Amplitude Modulation (QAM) is a technique where the combination of two amplitude modulated signal will be transmitted along with pulse amplitude modulation into a single channel. This helps in doubling the effective bandwidth. It has a high noise tolerance and a superior anti-noise performance. It is most suitable to work in environments which have a large signal-to-noise ratio and band-limited value [6]. QAM (512) is the modulation scheme used.

Implementation is done in MATLAB software.

II. Methodology

2.1 Algorithm

1. Start
2. Read the image that has to be transmitted.
3. Change the scale of the image and resize it into standard 256×256 size to fit the standards for transmission.
4. Import the data from the image.
5. Encrypt the grayscale image data using the RSA algorithm.

6. Display the encrypted data; resize the data according to the encoding scheme by padding zeros.
7. Import the encrypted data and feed it to the RS encoder.
8. Encode the data using RS (511,201) encoding scheme.
9. Display the encoded image.
10. Modulate the encoded image using QAM modulator with the order $M = 512$.
11. Add the noise to the modulated image. This is to demonstrate error detecting and correcting capabilities.
12. Feed the noisy image to the QAM demodulator with order $M = 512$.
13. Display the decoded image.
14. Resize the decoded image to the standard size by removing padded zeros.
15. The resized decoded image is decrypted by making use of the RSA decryption Algorithm.
16. Display decrypted data. This is the output at the destination.
17. Stop

2.2 Proposed method

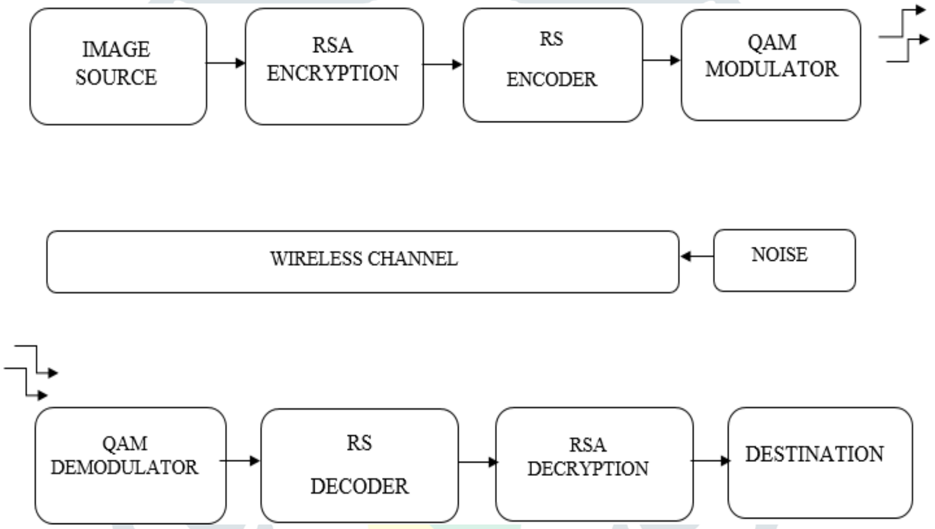

Figure 1. Block Diagram for Efficient and Secure Transfer of Data over Wireless Network

Figure 1 shows the block diagram consists of image source, RSA encryption, RS encoder, Quadrature amplitude modulator, wireless channel, quadrature amplitude demodulator, RS decoder, RSA decryption, and destination.

a. Image Source:

A source is a system that generates the message data which is used for communication. The input message data is considered to be a grayscale image. The image is a pictorial description of something. It represents anything, human, objects or scenes. It is a picture generated on an electronic display like a computer or mobile screen. An image is two-dimensional signals which can be represented in terms of a mathematical function (x, y) where x and y are the two Cartesian co-ordinates that represent the horizontal and vertical values. The numeric value of the function (x, y) at any point in the image gives the pixel values at that particular point.

b. RSA Encryption:

The pixels of the input image are converted into double value before undergoing the encryption process.
RSA encryption is an example of public key cryptosystem techniques. In this technique, 2 different keys are used; one is used for the process of encryption and the other for decryption. They are labeled as Public and Private Keys [1]. The RSA technique is a block cipher where the plaintext and cipher text are integers. This scheme is one of the most widely accepted public key encryption schemes. Both sender and receiver must know the value of ‘n’. A public key ‘e' is used for encryption which only the sender knows and the private key$'d$’ is used for decryption which only the receiver knows [2]. The public key pair is given by $\{e, n\}$. The private key pair is given by $\{d, n\}$.

The encryption is,

$$C = M^{e} mod n \text{ ………………..(1)}$$

where M is the message to be transmitted, C is the cipher text.

This results in an encrypted image. This image is then converted to unsigned 8 integer type where the maximum value is 255. This restricts the pixel values to 255 in the encrypted image. This resultant encrypted image is converted to double type and later sent as the input to the RS encoding scheme.

c. Reed Solomon Encoder:

The encrypted image is also a 256×256 size image which consists of 65536-pixel values. Each of these pixels is in encrypted form. Each encrypted pixel must be encoded.

We know that the pixel values range from 0 to 255. To encode using RS coding scheme appropriate (n, k) values must be selected. The RS encoder considers 'k' message bits, attaches $2t$ parity symbols to 'k' bits of input information to result in 'n' bits. RS codes are a subset of BCH codes [5]. RS codes are constructed using Galois field arithmetic. The Galois field with q elements is usually denoted as GF (q). Since the message data is considered for the encoder is a 256×256 encrypted image with maximum pixel value as 255. Here, GF (512) i.e. GF (2^9) is considered where 2 is the prime number and 9 is a positive integer [3]. In this case, n = 511. Now, an appropriate k value must be selected. The Reed Solomon codes are mainly used to correct the burst errors that are caused in the wireless channel. When the data like the image is considered, the quality of the data that will be retrieved is important hence the error correction % of the RS coding scheme must be high [4]. The error correction and detection and correction capability is an important factor which decides the efficiency of data received. The number of parity bits added to the message bits plays a prominent role in deciding the error correction percentage. The number of parity bits that are added depends upon 'n' and 'k' bits.

The no of parity bits = n – k.For RS (511, 201) the 't' was found to be 155 which means it can correct up to 155 errors. The 2t parity bits are added to k message bits to lead to n bits codeword.
Before feeding the encrypted image data into the encoder, the image needs to be resized. The total number of pixels was 65536. Since the k value that is selected is 201, then it is easy to encode. A block of k bits (k = 201) is considered and should be multiple of k i.e. (201). Hence, the encrypted image data must be padded with zeros. The generator polynomial was generated using this primitive polynomial. The generator polynomial is a GF (2^9) array. The elements are the Galois field elements. The input before undergoing RS encoding is first converted to Galois field elements. After conversion, it is encoded using RS (511,201) scheme.

The resultant encoded data is converted to double to feed it, to the QAM modulator.

d. Quadrature Amplitude Modulation (QAM):

Here, 512-QAM theme is employed. This is because as the particular method of modulation goes, the theme of QAM doesn't deviate from the norm. As directed by the method of modulation, a particular side of the carrier signal is modified with relation to the information. This remodeled response is sometimes sinusoidal in nature. The 'quadrature' in QAM comes from the very fact that the carrier wave is the sum of two waves of the identical frequency. The two parts, however, vary from one another in terms of the part, they're orthogonal to every different i.e., they're 90° out of part with one another (in Quadrature). The two parts of the carrier are so competently known as "I" or the in- phase part, and also the "Q" the Quadrature part. Every part is amplitude modulated in respect to the message signal. The input signal m(t) is fed into a flow splitter and sent to the impulse generator. These signals are then used to modulate the carrier [6]. The signals are then added and processed as per requirement. Then it is amplified as required.

e. Noise:

The image post modulation may be transmitted over a wireless network provided by the antennas. To demonstrate the practical aspects of the wireless transmission we tend to introduce noise to the modulated image. The noise is supplemental to the image indiscriminately picture element values. The pixels are chosen indiscriminately and therefore the worth is modified to black or white. The mechanism imitates the Salt and Pepper noise. The noise is additionally introduced to demonstrate the error detection and correction capabilities of the RS encoding scheme.

f. QAM Demodulator:

The demodulator is the initial block on the receiving side of the setup. The order of the demodulator, similar to the modulator is 512. The demodulator performs the reverse operation as the QAM modulator. The signal enters the receiver system, which is then split into two parts. Each component is applied to the mixer. One half has the in-phase local oscillator applied whereas the other has the quadrature component. An additional requirement for the demodulator is to derive a local oscillator signal to be exactly on the required frequency for the signal. Recovery of the phase of the carrier is important otherwise the bit error rate of the data will be compromised [6].

g. RS Decoder:

The Reed -Solomon decoder block is the next block in the system. The scheme used is RS(511,201) . It takes the demodulated image as the input which is a matrix of order 109×1533. The demodulator output is fed to the RS decoder to obtain the decoded image which is of the order 109×601. The salient feature of the RS encoding scheme is demonstrated in this block where the noise added to the modulated image is detected and corrected. In theory, the RS decoder considers the incoming message as a polynomial [3]. The received polynomial R(x) is combination of the transmitted polynomial T(x) and therefore the error polynomial E(x) i.e.

$$R(x) = T(x) + E(x)\text{………………..(2)}$$

The decoder's task is to identify and correct E(x) in R(x) to obtain T(x) is given by

$$T(x) = R(x) + E(x).\ \text{……………….(3)}$$

The input to the decoder is first considered row-wise where the entire row is divided into an individual block of length n. These individual blocks of length n are then represented in terms of Galois field elements [5]. This is the input to the RS Decoder which detects errors and corrects them. The amount of errors which can be detected by the scheme are t = n-k [4]. The number of errors it corrects is t/2.The output is k message bits. The output is a matrix of dimensions 109×1533. Before feeding the image to the decryption block, it has to be resized into the standard 256×256.

h. RSA Decryption:

Once the received image data is demodulated, successfully decoded, it must be decrypted using the RSA algorithm to produce the image. This image is then compared to the original image to know if there was successful retrieval of the image at the receiving end. Any errors that were added in the wireless channel was detected, located and corrected at the RS decoder. Now the output from RS decoder is the input for RSA decryption block. The reshaped decoded image data undergoes RSA decryption to give the original image.

RSA algorithm utilizes private key to decrypt the ciphertext. Private Key d is privy only to the receiver. The private is a pair in $\{d,\ n\}$.By using the equations, d is calculated.

$$d\ \times\ e\ \ =\ 1.mod\Phi(n)\ \text{………………..(4)}$$

$$d\ \ =\ e^{-1}(mod\Phi(n))\ \text{………………..(5)}$$

Result of the decryption block is decrypted image that is similar to the input grayscale image which was sent to the RSA encryption block.

$$M\ \ =\ C^{d}modn\ \text{………………..(6)}$$

The decrypted output and the original grayscale input are compared to one another to check for any discrepancies. If the difference is 0 then the transmission is efficient and successful. The retrieved image is then sent to the destination

i. Destination:

The destination is the last stage of the receiving part of the entire system. The destination is the system to which the information is supposed to be sent. The destination, like the source, is a digital system which intercepts the digital image. The image received after decryption is the resultant image. This image is in grayscale and the dimensions are 256×256. The source image can be grayscale or RGB image with any kind of dimensions but, before the encryption process, the input image is scaled down to grayscale with standard dimensions 256×256. This input that is given to the encryption block is the output we obtain after the decryption process. This is the image obtained at the destination. The destination is a digital system which can manipulate and receive the decrypted image. Further developments can be done to change the scale of the image and resize it. Thus the destination block is the end-user system that receives the image that is transmitted.

2.3 Software Requirements

MATLAB is a high-level computer programming language which allows one to create functions, store the files and analyze data. It is easy compared to other platforms as it is closer to human understandable language.

The version used is MATLAB version 9.6 [R2019a]. We use GUI for a smooth user interface. GUI stands for Graphic User Interface is a type of software which works with of click or point of contact between and the user. They are accessible by using a mouse or a pen. The main advantage of this is one can use all the programs and algorithms without having the knowledge of additional commands.

III. Results

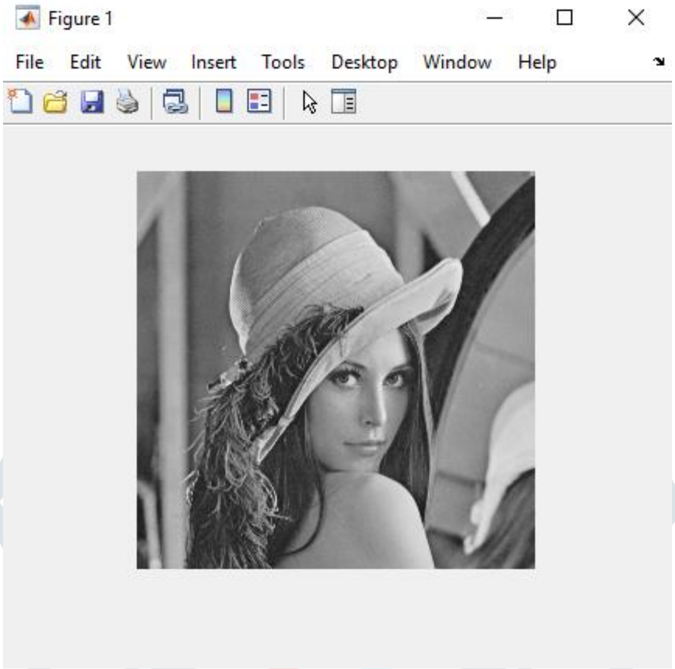

Figure 3.1.Input Grayscale Image

Figure 3.1 depicts the input image given to the encryption block. Here, the input taken is the standard Lena image. The image is grayscale with the standard 256×256 dimensions. The input image can also be taken as a color image or a multispectral image which can be scaled to grayscale and resized to a standard 256×256 since these are the requisites of our system.

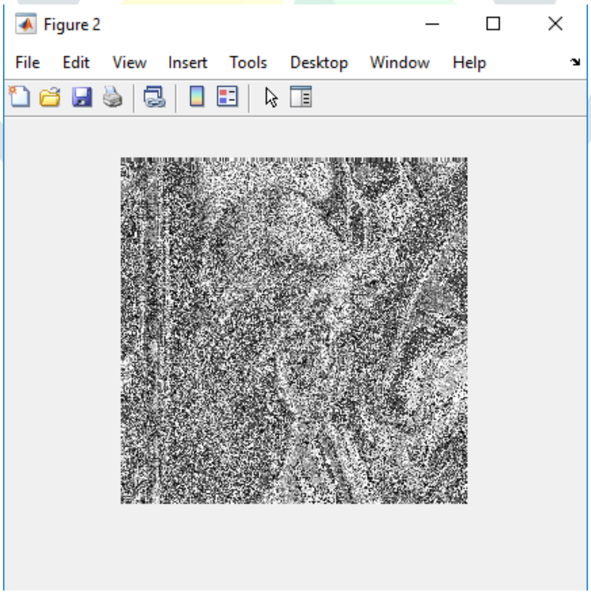

Figure 3.2. RSA Encrypted image

Figure 3.2 shows the encrypted image. It is a matrix which has dimensions 256×256. It is obtained by the RSA encryption algorithm. This image is resized according to the RS (511, 201) encoder and then is encoded.

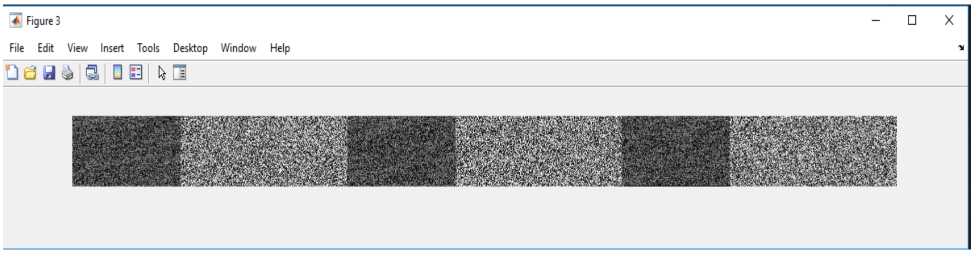

Figure 3.3. RS Encoded Image

Figure 3.3 shows the decoded image. The encrypted image is resized into a 109×603 matrix and fed to the encoder. The encoder considers each row and divides it into blocks having k values. The decoder output happens to be a block with 511 bits. The dimensions of the image are 109×1533.

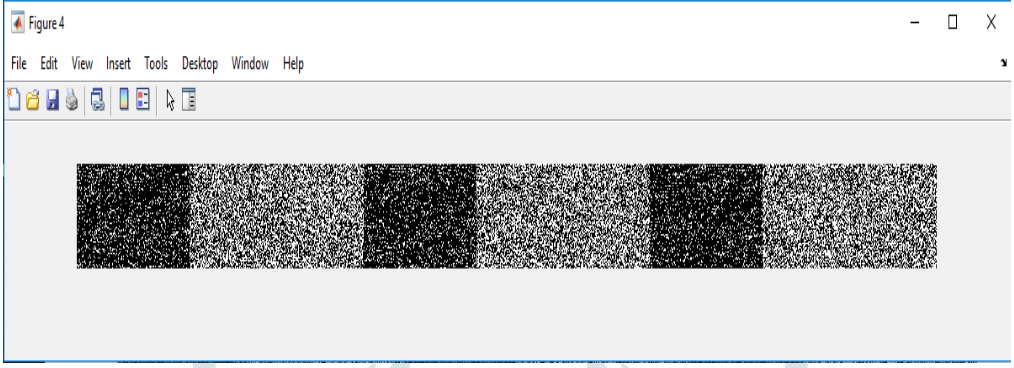

Figure 3.4. Image modulated by QAM Modulator

Figure 3.4 shows image after QAM modulation. The encoded image is fed to a digital QAM modulator of order 512. The dimensions of the image are 109×1533.

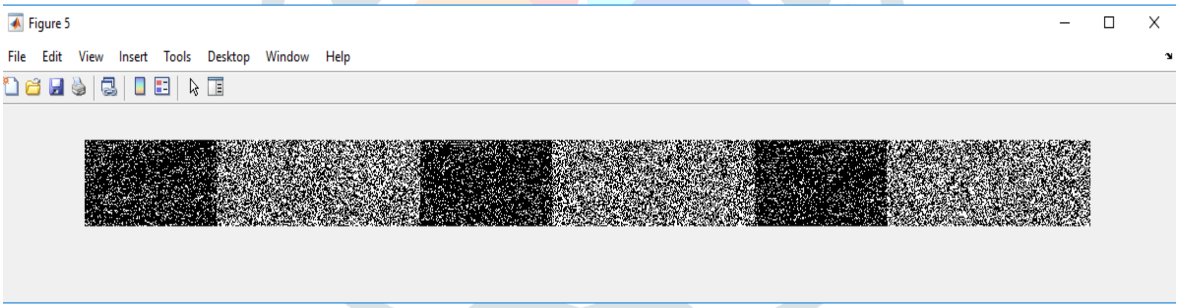

Figure 3.5. Image after the addition of Noise

Figure 3.5 shows the resultant image after the noise is added. To demonstrate the error detecting and correcting capabilities, noise is introduced to the image at random pixels. The value of the pixels is changed to either 0 or 255.The mechanism apes the Salt and Pepper noise. This noisy image is fed to QAM demodulator of order 512. The noise is added to model the effect of noise during transmission in a wireless channel. It is also added to demonstrate the error detecting and correcting capabilities of RS (511,201) encoding scheme.

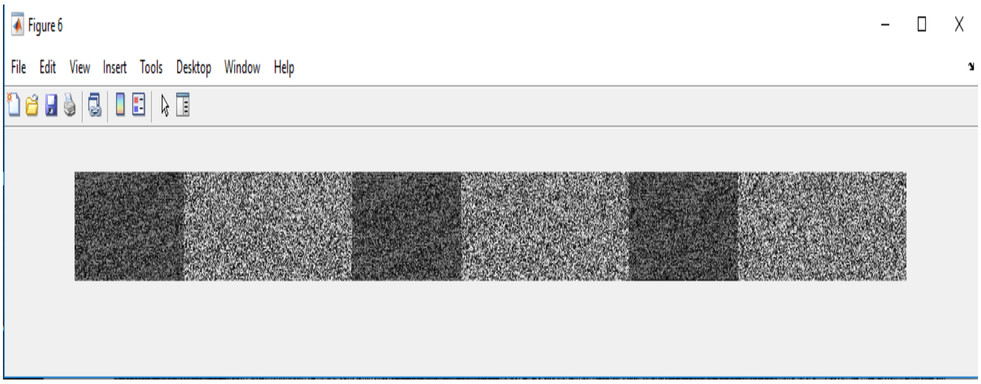

Figure 3.6 QAM Demodulated Image

Figure 3.6 shows the demodulated image. The noisy image is fed to the demodulator. The output of the demodulator is fed to the decoder.

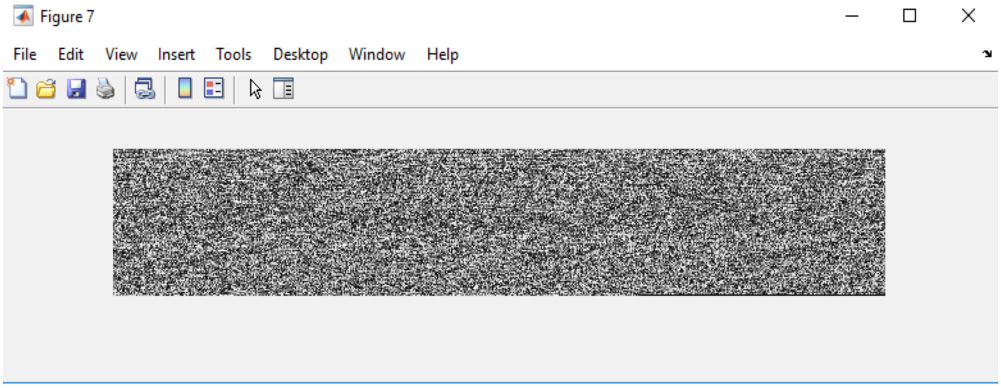

Figure 3.7 RS Decoded Image

Figure 3.7 shows the decoded image. The demodulated image is fed to the RS decoder. It considers each row and divides the row into individual blocks of length ‘n' and it is decoded. It gives the output of ‘k’ bits. The resultant image is of dimensions 109×603. The output of the decoder is resized to standard 256×256. This resized image is fed to the decryption block using RSA decryption algorithm.

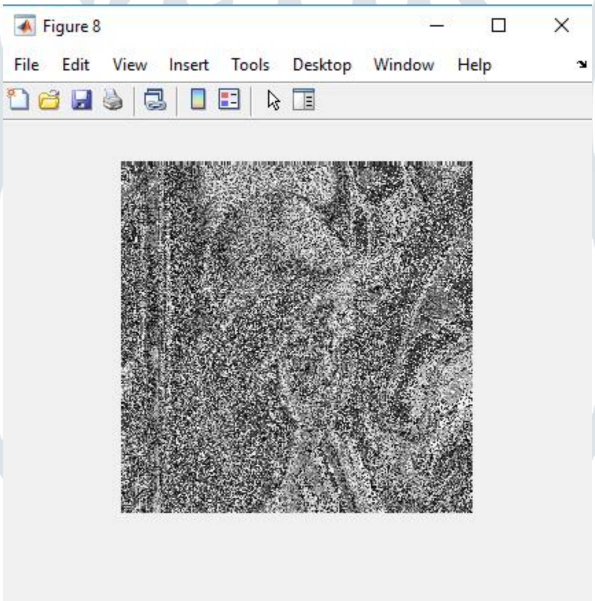

Figure 3.8 Resized Decoded Image

Figure 3.8 shows the resized decoded image. The decoded image is of 109×603, which cannot be fed to the decryption block. The image therefore has to be resized and the padded zeros are supposed to be removed. Post resizing, the image to a standard 256×256, it will look like the one in the figure. This image is then given as input to the decryption block.

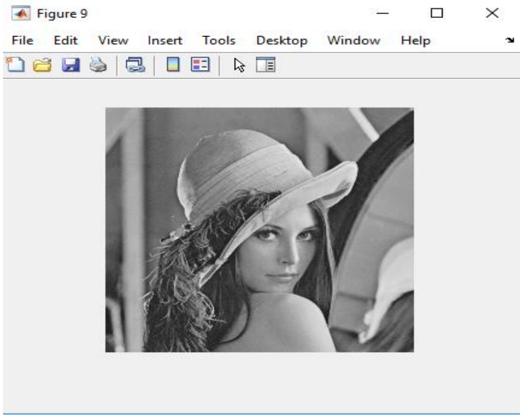

Figure 3.9 RSA Decrypted Image

Figure 3.9 shows the decrypted image. It is the same as the original input. The size of the input of the decryption block is 256×256. The output can be compared to the original image to find any deviations if present.

IV. Conclusion

In this fast-paced world, efficiency holds key importance in any mundane process of our daily lives. The process of data transfer has been given an efficient do over. It is done so by introducing the process of cryptography and encoding. The encrypting algorithm is the RSA scheme, while the encoding is done by the RS encoding scheme. They are chosen for their advantages over their competitors. RSA encryption is superior to certain basic encryption algorithms in terms of key management. The RS encoding scheme is adopted for its burst error detecting and correcting capabilities. Both these processes serve as improvements to the goal that is efficient data transfer. It is basically a twofold approach. Efficiency in encryption is measured in terms of the security of the data transferred, whereas the process of encoding measures efficiency based on the effect of noise in the channel on the transmitted image. The data transmitted thus gets two layered protection at the source and from channel interference. The modulation is done in order to aid transmission over a network. Quadrature Amplitude Modulation (QAM) scheme based on the applications of this project is found to be very efficient. Thus, this type digital modulation method is adopted.

V. Future Scope

The proposed method comes with ample future scope. The approach utilized in this project is a very basic one which can be used as the basic skeletal structure for improvements. From the view point of data, the type of data considered is an image. That can be graduated into different kinds of images like multispectral image, IR image, hyper spectral image, etc. A further enhancement can be done by using videos as the input. In terms of the encryption algorithms, an improvement would be using other sophisticated and efficient encryption algorithms like AES, DES, or elliptic curve cryptography. Similarly, encoding schemes like BCH, LDPE, Turbo code, etc. can be used to replace the RS encoding scheme. Modulations schemes like OFDM can be used as a replacement. Since the output is a modulated image, it is ready for transmission. The project can be further improved by creating a wireless network that is supported by antennas. Antennas can be designed and parameters can be varied to find maximum efficiency in terms of data transmission Many steps like these can be adopted to improve this project further.

References

[1] Shankha Mukherjee; Souvik Sinha; Shakya Chakrabarti; Tamal Mukhopadhyay, “A meticulous implementation of RSA Algorithm using MATLAB for image encryption”, 2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech)

[2] S. Anandakumar, “Image Cryptography using RSA Alogrithm in Network Security”, Research Scholar, School of Computer Science, Engineering and applications, Bharathidasan University, Tiruchirapalli, IJCSET, September 2015, Vol 5, Issue 9,326-330

[3] Phat Nguyen Huu, Vinh Tran-Quang and Takumi Miyoshi, “Multi-hop Reed-Solomon encoding scheme for image transmission on wireless sensor networks”, Fourth International Conference on Communications and Electronics (ICCE), 1-3 Aug. 2012

[4] Nir Drucker, Shay Gueron and Vlad Krasnov, “The comeback of Reed Solomon codes”, 2018 IEEE 25th Symposium on Computer Arithmetic (ARITH), pp 125-129, 25-27 June 2018

[5] Sanjana P. Choudhari and Megha B. Chakole, “Reed Solomon code for WiMAX network”, 2017 International Conference on Communication and Signal Processing (ICCSP), pp 176-179, April 6-8, 2017

[6] Dayong Hu, “A simulation method of 16QAM modulation and demodulation based on Matlab platform”, 2017 7th IEEE International Symposium on Microwave, Antenna, Propagation, and EMC Technologies (MAPE) pp172-175, 24-27 Oct. 2017