

# Designing secured data using a combination of JPEG2000 Compression, RSA Encryption and DWT Steganography

Sayli S. Relekar<sup>1</sup>, Prof. V. B. Raskar<sup>2</sup>

<sup>1</sup>Sayli S. Relekar, Dept of Electronics and Telecommunication, Imperial college of Engineering and Research, Maharashtra, India

<sup>2</sup>Prof. V. B. Raskar, Dept of Electronics and Telecommunication, Imperial college of Engineering and Research, Maharashtra, India

\*\*\*

**Abstract** - The paper describes the combination of different method use to secure the data. The cryptography and steganography technique are used to secure the data. Cryptography technique is use to encrypt the data. Steganography technique is use to hide the data within the selected image. . For that, we first substitute the original message by using the fourteen square substitution algorithms. After the substitution of text, we then encrypt this text message using RSA algorithm. The encrypted message compressed by JPEG 2000 (Huffman coding) method, so it will reduce the size of the message that will be inserted and increase the capacity of messages that can be inserted. Messages that have been compressed and encrypted, is then hidden by DWT (Discrete Wavelet Transform) techniques. With the incorporation of encryption techniques, steganography, and compression, the acquired information is more secure and its capacity is larger. At the receivers end, same operations are performed to decrypt the original message in reverse order. It is found that here we are using the double ciphering techniques which makes the system very robust and secures it from known hacking attacks. It makes very difficult for the intruders to hack the image and then decrypt the message in a feasible amount of time thus securing it from many known network attacks

**Key Words:** Cryptography and steganography, JPEG2000 Compression, DWT, RSA encryption.

## 1.INTRODUCTION

Now a days network security is very essential in encrypting the data and decrypting the data. Hence there are various technique used for network security. Most commonly the cryptography is used for the security. And there many other technique used for security. As to transmitted the secret data only cryptography is not essential for encrypting and decrypting the data. So in this paper we are doing dual encryption and for testing this encryption we are Applying some parameter as they are Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER). For dual encryption we using two different algorithm as they are fourteen square algorithm and RSA algorithm.

SG is used for the data hiding technique. SG means cover and grapy means writing. SG is mainly used for the image and audio. In this paper SG is used for the video processing. For data hiding in video, the video is divided into frames of images. And the frames of images is selected within them and in one of the image the data is hided. In such a way the video processing is applied.

The word Steganography is derived from the Greece words Stegos means cover and Grafia means writing. Steganography can be achieved by using image, audio, video carriers. The most flexible and efficient way to use it is with help of images, hence in our software, we are using it in form of image. Encryption and steganography are the preferred techniques for protecting the transmitted data , as a result, there are various encryption systems to encrypt and decrypt image data, and it can be argued that there is no single encryption algorithm satisfies the different image types . Data exchange is a good example of an application that uses encryption to maintain data confidentiality between the sender and the receiver. In this paper, steganography is used to hide information to perform encryption. Steganography techniques are getting significantly more sophisticated and have been widely used. The Steganography techniques are the perfect supplement for encryption that allows a user to hide large amounts of information within an image.

Thus, it is often used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the hidden information before decryption take place. The problem with cryptography is that the encrypted message is obvious. This means that anyone who observes an encrypted message in transit can reasonably assume that the sender of the does not want it to be read by casual observers. This makes it possible to deduce the valuable information.

In this project we are hiding the text message in the color image using the encryption technique. In this we are taking the color image in that we are going to hide the text message. The encryption of this text is first process by the 14 square algorithm. And after encrypting by 14 square algorithm we are again encrypting by the RSA encryption technique. In this project we are dual encryption is done for higher level of security. After

encryption process we are going to compression technique, which is JPEG2000 compression, in this the size of the image is compress.

## 2. CRYPTOGRAPHY AND STEGANOGRAPHY COMBINATION

### 2.1 CRYPTOGRAPHY

Cryptography is the art and science to encode the messages to make them unreadable. This message is unreadable to the other but the message is only readable to the sender and receiver. The cryptography is use to encrypt and decrypt the data between two parties. Cryptography provide the authentication key for verifying the identity of sender and receiver. Cryptanalysis is the reverse engineering of cryptography. There are various ways to classify the cryptographic algorithms. The three types of algorithms are:

- (1) Secret key Cryptography: Uses only one key for both encryption and decryption.
- (2) Public Key Cryptography: Uses different key for encryption and different for decryption.
- (3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

### 2.2 STEGANOGRAPHY

Steganography is derived from the Greek Steganos (hidden) and graphein (writing). Steganography means cover writing. Steganography is a art and science of hiding messages into a image or video files in a way that actually don't know any one, only the sender and the receiver. The steganography, hides the secrete information in the media files such as the image, video, audio file. There different types of the steganography. They are as follows:

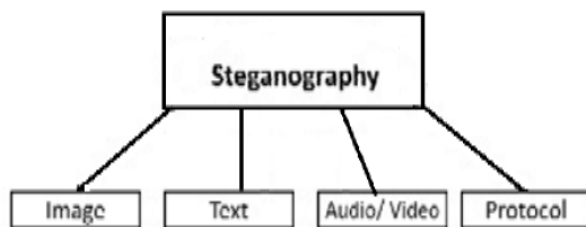


Fig. 1. Types of steganography

Steganography is used for almost all media file formats, but these file are with a high degree of redundancy . Redundancy is use to defined as the bits of an object which provide accuracy for the object's use and display. Image and audio files are especially encrypted with there necessary, it cover the secrete information in the media files that is, it hide the information in the media file. Image file are mostly used in steganography for hiding data.

#### 2.2.1 SPATIAL DOMAIN STEGANOGRAPHY :

Spatial domain technique is mostly used for Least Significant Bit (LSB) . The least significant bit is use to embedded bits of the message into the LSB of the pixel image. But the problem with this technique is that if the image is compressed, the data inserted may be lost. Thus, there is a fear for the loss of data that might have sensitive information.

#### 2.2.2 FREQUENCY DOMAIN STEGANOGRAPHY:

In frequency domain the message is embedded in the image. In frequency domain the embedded data which is the hidden data, this data is spread across the image and this data is more stronger in the image area. There are various techniques that change the image from spatial domain to frequency domain. 2D discrete cosine transform is usually used in the frequency domain. In frequency domain there are various discrete transform are used such as the discrete wavelet transform, discrete cosine transform, discrete Fourier transform.

The wavelet transform works on the time frequency which provide signal. In this paper we are applying discrete wavelet transform and even inverse wavelet transform. Discrete wavelet transform is use to embedded the secrete data in the original image and to embedded the stego image we use the inverse wavelet transform to regain the original image. The image pixel consist of the low level and high level pixel. The discrete wavelet transform is use to hide the data in low level(LL) pixel in image. The low level pixel are the integer number and the high level(HL) pixel means floating point.

In discrete wavelet transform it embedded integer to integer. The wavelet transform is more efficient to lossless compression. And in this project we are using the JPEG2000 compression which is the lossless compression. Thus to get the perfect output the discrete wavelet Transform and the inverse wavelet transform is used in combination of encryption and decryption.

The discrete cosine transform is also used for hiding secrete data. The discrete cosine transform is use to divided the image into  $8 \times 8$  blocks and each block is transform is done. It set the image pixel according to the image frequency value. In discrete cosine transform it embedded only the high frequency bit or coefficient. In the blocks after discrete cosine transform DCT, the pixel position of 8th row and 8th column (8,8) is use to change the  $\delta$  for hidden data bit to 1, and change to  $-\delta$  for hidden data bit to 0.  $\delta$  represents the positive value to hide the data bit. And the  $-\delta$  represent the negative value to hide the data bit.

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind

of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

### 2.3. CRYPTOGRAPHY AND STEGANOGRAPHY COMBINATION

Working only on cryptography or the steganography is not sufficient, because the cryptography and the steganography technique are used for the security. If any one technique is used for the security it will not help to secure the confidential data. The role of the cryptography is to encrypt and decrypt the information. And the role of steganography is to hide the confidential data into the image. So the combination of cryptography and steganography is more efficient than to use anyone technique. In cryptography, the attacker can hack the confidential data easily. But when the steganography is used the attacker is use to first identify the secret embedded data and then the attacker is use to hack the data.

However, it is good practice to use Cryptography and Steganography technique together for additional multiple layers of encryption. The combination of the data encryption is done by a software and then embed the information in the cipher text that is image, video, audio or any other media file with the help of steganography key. The combination of cryptography and steganography technique will enhance the security level of the secrete data embedding. The combination of these two technique will satisfy the requirements such as the capacity, security and robustness to secure the data transmission.

The explanation of the figure shown below is the combination of the steganography and cryptography technique. The first block consist of the plain text, the plain text means the secrete data which can be a alphabet, numbers or any special character. The plain text is then applied to the encryption block. There are various encryption technique which are used to encrypt the data such as the 14<sup>th</sup> square encryption, RSA encryption etc. The encryption block will encrypt the plain text and it will convert into the cipher text. Then the encrypted data is pass to the cipher text.

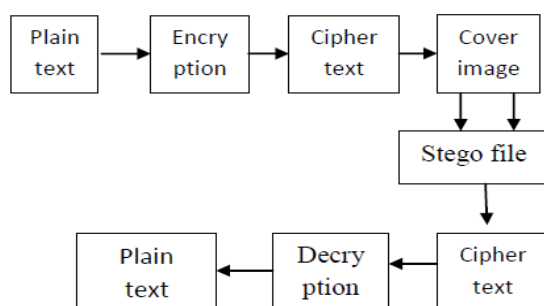


Fig. 2.Cryptography and steganography combination

The cipher text is the encrypted data which is unreadable to the attacker. The cipher text is then applied to the cover image. The cover image is the image in which the data is hidden with the help of the steganography technique. And hence the data is hidden in the stego image. To get the original message back we have to reverse the process that is decrypt the stego image. And at the output we get the original image and secrete data without disturbance.

### 3. PROPOSED SYSTEM

#### 3.1 RSA ALGORITHM

RSA algorithm was introduced by three researchers from MIT (Massachusetts Institute of Technology), namely Ron Rivest, Adi Shamir, and Len Adleman in 1976. RSA encryption and decryption process is based on the prime numbers and modulo arithmetic. The encryption and decryption keys are integers. RSA algorithm work on the public key. The encrypted key is kept secret and is not known to anyone (so-called public key), but kept secret key for decryption. Decryption keys is made up of multiple prime integers together with the encryption key. If we have to find the decryption key, we must factorize a composite number into prime factors. But factorizing the nonprime numbers into prime number is not easy. The RSA algorithm is efficient to find the factor it. The large number are more difficult to get there non prime number factoring. The RSA algorithm is as follows.

RSA algorithm as follows:

1. p and q are primes (secret)
2. n = pq (not secret)
3.  $\Phi(n) = (p - 1) (q - 1)$  (secret)
4. e (encryption key) (not secret)
5. d (decryption key) (secret)
6. m (plain text) (secret)
7. c (cipher text) (not secret)

RSA algorithm is based on Euler's theorem which states that :

$$a\phi^n \equiv 1 \pmod{n} \dots \dots \dots (1)$$

a must be prime number to n

$\phi(n) = n(1 - 1/p1)(1 - 1/p2) \dots (1 - 1/pr)$ , where p1, p2, ..., pr are the prime number of n.

$\phi(n)$  is a function that determines how many of the numbers 1, 2, 3, ..., n which are relatively prime number to n. Based on the

nature of  $ak \equiv bk \pmod n$  for an integer  $k \geq 1$ , then the equation (1) can be written as :

$$a^k \phi^{(n)} \equiv 1^k \pmod n. \dots \dots (2)$$

$$\text{or } a^k \phi^{(n)} \equiv 1 \pmod n$$

So that encryption and decryption are formulated as follows:

$$E_e (m) = c \equiv m^e \pmod n. \dots \dots (3)$$

$$D_d ( m ) = m \equiv c^d \pmod n. \dots \dots (4)$$

Algorithms which generate the key pair :

- Choose any two prime numbers , p and q
- Calculate  $n = pq$  (preferably  $p \neq q$ , because if  $p = q$  then  $n = p^2$  so p can be obtained by numerical square root of n)
- Calculate :
- $\phi(n) = (p - 1)(q - 1)$  (5)
- Select the public key , e which is relatively prime to  $\phi(n)$
- Generate a private key using the equation :  $ed \equiv 1 \pmod{\phi(n)}$

#### 4. IMPLEMENTATION OF SYSTEM

##### 4.1 JPEG2000

JPEG2000 is first international standard of continuous tone still image compression and coding. It is very popular for the still image and it can be transfer over the internet and these still image can also be store in the devices. First, JPEG encoded images show severe blocking drawback at a low bit rate. This problem is due to block-based DCTs, which are discussed earlier. JPEG dose not support much to the spatial domain and SNR quality. The quality of the JPEG image is not so good and it dose not reconstruct the image properly. Hence to overcome these drawback the advance version was introduce that is JPEG2000 in 1996.

Fig. 3.JPEG2000 encoder block diagram

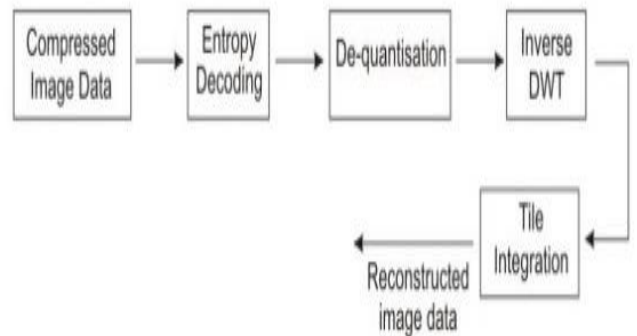
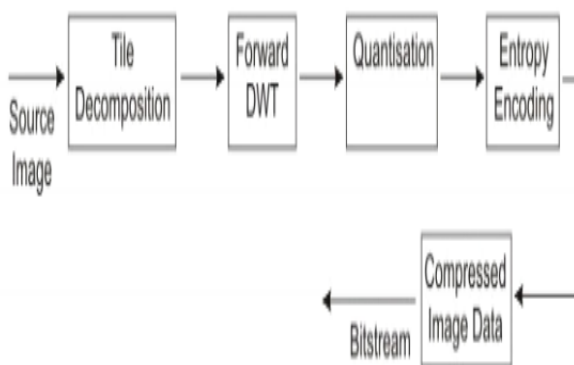


Fig. 4.JPEG2000 decoder block diagram

The JPEG block diagrams is mostly same as the JPEG2000 but the difference is that the JPEG2000 consist the discrete wavelet transform block rather than discrete cosine transform. Firstly the source image is applied the source image means the original image. The source image is then applied to the tile decomposition block. The tile decomposition block work on the source image, the source image is divided into component and these component is divided into tile.

These tile are then applied to the discrete wavelet transform (DWT). The discrete wavelet transform is use to transform the bit pixel in the image. And these bit are then applied to the quantized block. The bit is quantize and then it is applied to the encoded block. The encryption block is used to encrypt the bit. These encrypted bits are then applied to the compress block. The compress block is use to compress the bit and output of compress block is the compress bit stream.

##### 4.2 14<sup>th</sup> SQUARE ALGORITHM

In the earlier paper the twelve square cipher substitution is represented which includes only lower case alphabets, numbers and some special characters. This is extended in to fourteen square substitution ciphers to include numerals, upper and lower alphabets and all special characters including space bar which are present on keyboard. At first, the fourteen-square substitutes the alphabets, digits and special characters so it is less susceptible to frequency analysis attacks. It uses eight 9 by 6 matrices each arranged in a square, as shown in figure-1. Each of the 9 by 6 matrices contains the letters of the alphabets (upper case and lower case) and another six 6 by 7 matrices arranged in a squares for digits and special characters, as shown in figure-2. All the special characters from your desktop/laptop keyboard are included in this figure

Square1: We have taken fifty two alphabets and two special characters, out of which twenty six are capital letters and

twenty six, are small letters. In each row we have arranged nine alphabets and each column contains six alphabets.

Square 2: is made from square- 1 by taking the first row of the square-1 to sixth row place and other rows one position up.

Square 3: is created from square 2 by taking the first row of square 2 to sixth row place and other rows are position up.

Square 4: which created from square-3 by taking first row of square-3 to sixth row of square-4 and other rows are position up.

Square 5: we have converted rows into column and interchanged first and last alphabets.

Square 6 to 8: by taking first row of previous square to sixth row and other rows one position up.

Square 1	Square 2	Square 3	Square 4
stuvwxyzA	BCDEF GHI J	KLMNOPQRS	TUVWXYZ@?
BCDEF GHI J	KLMNOPQRS	TUVWXYZ@?	abcd efghi
KLMNOPQRS	TUVWXYZ@?	abcd efghi	jklmnopqr
TUVWXYZ@?	abcd efghi	jklmnopqr	stuvwxyzA
abcd efghi	jklmnopqr	stuvwxyzA	BCDEF GHI J
jklmnopqr	stuvwxyzA	BCDEF GHI J	KLMNOPQRS
Square 5	Square 6	Square 7	Square 8
ryEKQWagm	tzFLRXbhn	uAGMSYcio	vBHNTZdjp
tzFLRXbhn	uAGMSYcio	vBHNTZdjp	wCIOU@ekq
uAGMSYcio	vBHNTZdjp	wCIOU@ekq	xDJPV?fls
vBHNTZdjp	wCIOU@ekq	xDJPV?fls	ryEKQWagm
wCIOU@ekq	xDJPV?fls	ryEKQWagm	tzFLRXbhn
xDJPV?fls	ryEKQWagm	tzFLRXbhn	uAGMSYcio

Fig. 5. Plain Text and Cipher Text Table(Alphabets)

The plain text is read from left to right. If the character is alphabet it will refer to the figure-1, otherwise if it is a number or a special character it will refer to figure-2. While scanning the plain text the first alphabets plain text is in square-1 and its cipher is in same row and column location in square-5. The second alphabet, its plain text is in square- 2 and its cipher text is in same row and column location of square6. The third alphabet, its plain text is in square-3 and cipher text is in same row and column location of square-7.

The fourth alphabet, its plain text is in square 4 and its cipher text is in same row and column location of square-8 similarly fifth alphabet corresponds to square-1 and square-5, 6th alphabet corresponds to square-2 and square-6, 7th alphabet corresponds to square-3 and square-7 and so on. Secret message is combination of alphabets, digits and special characters. While scanning for the secret message, for the special characters and digits it will refer to the figure-2.

The special character (including digit), its plain text is in square-9 and cipher text is in same row and column location of square-12. For another special character(including digits) it follow the same procedure as mentioned for figure-1 characters

Square 9	Square 10	Square 11
0123456	789`~!`	#\$%^&* (
789`~!`	#\$%^&* (	) _ - + = { [
#\$%^&* (	) _ - + = { [	} ] ; : " ' \
) _ - + = { [	} ] ; : " ' \	< , > . € /
} ] ; : " ' \	< , > . € /	0123456
< , > . € /	0123456	789`~!`
Square 12	Square 13	Square 14
06 ! & + ; <	17 * = : ,	17 * = : ,
17 * = : ,	28 # ( { " >	28 # ( { " >
28 # ( { " >	06 ! & + ; <	39 \$ ) [ ' \
39 \$ ) [ ' \	39 \$ ) [ ' \	4 % _ ]   /
4 % _ ]   /	4 % _ ]   /	5 ~ ^ - ]   /
5 ~ ^ - ]   /	5 ~ ^ - ]   /	06 ! & + ; <

Fig. 6. Plain Text and Cipher Text Table(number and special character)









After this successful substitution of the plain text, again this cipher text will be encrypted by the one of the most secure encryption algorithm. For this we are using the RSA algorithm form encryption and decryption process and lastly the encrypted message will be embedded inside the image. The substituted image is then re-encrypted using the RSA in following way.

### 5. RESULT AND EXERIMENTAL OF THE

In cryptography, message gets encrypted and in Steganography, it gets embedded within the selected image. For that, we first substitute the original message by using the fourteen square substitution algorithm. After the substitution of text, we then encrypt this text message using RSA algorithm and 14<sup>th</sup> square algorithm. The encrypted message is then hidden within image by Least Significant Bit (LSB) method.

This image works as a carrier file and is sent to the receiver. At the receivers end, same operations are performed to decrypt the original message in reverse order. It is found that here we are using the double ciphering techniques which makes the system very robust and secures it from known hacking attacks. It makes very difficult for the intruders to hack the image and then decrypt the message in a feasible

**Table -1:** Output stego image and parameters

Input image	PSNR	MSE	Stego image
	67.57	0.011	
	66.63	0.014	
	66.27	0.015	
	66.52	0.014	

$$MSE = \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (x_{ij} - y_{ij})^2$$

Here  $y_{ij}$  denoted to the process pixel value  $x_{ij}$  denoted to the original pixel value, m and n denote to the height and width of the image.



**Fig. 7.**Input image



**Fig. 8.**Denoised image



**Fig. 9.**Output stego image

The comparative results of the different images and the two different parameters. To calculate the PSNR and MSE.

There are various parameter to analysis the efficiency of the image or the video. The parameters are set to identify the efficiency of an image.

### 5.1 PEAK SIGNAL NOISE RATIO (PSNR), MEAN SQUARE ERROR (MSE), BIT ERROR RATE (BER)

Peak signal noise ratio (PSNR) is use to test the image quality. PSNR is most commonly used for the image but in this paper we are Applying it to the video processing.

$$PSNR = 10 * \log_{10} \left( \frac{255^2}{MSE} \right)$$

Mean square error (MSE) is use to define the error. And it is defined as

Input Text :sudharson

fourteen square substitution Cipher Text :rE0kwsr?V

Rsa algorithm Cipher Text :00k0f000E

Processing time for Embedding in (ms):1.159862e-02

MSE:0.014121

PSNR:66.631997

**Fig. 10.** Output of the secrete data and parameters

## CONCLUSION

The simulation design of securing data using a Combination of JPEG2000 Compression, RSA Encryption, and DWT Steganography is more efficient than the LZW compression. As the capacity of the compressed data is more in JPEG2000. And further comparison with the other encryption technique to secure data more efficiently

## REFERENCES

- [1] Gandharba Swain, Saroj Kumar Lenka, "Steganography using the Twelve Square Substitution Cipher and Index Variable", IEEE transactions on Image Processing, 2011.
- [2] Saleh Saraireh. "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.
- [3] Geeta Kasana , Kulbir Singh "Steganography Technique for JPEG2000 Compressed Images Using Histogram in Wavelet Domain" Vol.8, No.6 (2014).
- [4] Manoj, I. V. S., "Cryptography and Steganography". International Journal of Computer Applications (0975-8887), Vol.1, No.12, 2010.
- [5] Saleh Saraireh. "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.