

AN IMPROVED CRYPTO-STEGANOGRAPHIC TECHNIQUE FOR DATA HIDING USING MODIFIED LEAST SIGNIFICANT BIT AND RIVEST SHAMIR ADLEMAN ALGORITHMS

¹*Ogunleye G. O., ¹Ayogu B. A., ¹Ayeni O. T.

¹Department of Computer Science, Federal University, Oye-Ekiti, Ekiti State, Nigeria.
Present/Permanent Address: Department of Computer Science, Federal University, Oye-Ekiti, Ekiti State, Nigeria

*Corresponding author E-mail address: gabriel.ogunleye@fuoye.edu.ng (G.O. Ogunleye).

ABSTRACT

This study is aimed at developing an improved LSB technique by overcoming the standard LSB technique's high imperceptibility and transparency, especially in JPEG and BMP formats which are the characteristics of a truly secure and reliable security technique for remote data transmission. The creation of a modified LSB (mLSB+DWT) algorithm combined with RSA would enhance secured data transmission and image security. The standard LSB was modified to create a balance between the algorithm's exploration and exploitation stages so as to improve quantity solution in detecting high energy coefficient (optimal wavelet coefficient) of DWT and to resolve conflicting requirements of different parameters and properties of digital images. The techniques achieved improved Average difference, Mean Square Error (MSE), Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), Image Fidelity and Normalized Cross Correlation (NCC), indicating a higher quality measurement between the original and compressed images using different formats

Keywords: Rivest Shamir, Adleman, Steganographic, Data, Bit

INTRODUCTION

In the world of today, passage of data through the internet is continually growing due to the ease and speed of data delivery to several destinations which has made many individuals and business personnel transfer very important data across the internet. Over time, there have been growing concerns about security and privacy of data on the internet. Even, some emerging security applications are now being compromised by more powerful attacks including the Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks (Amir, 2021), Advanced Persistent Threats and Malicious Ransomwares (Apau and Adomako, 2017).

These challenges have made it incumbent that security of data on the internet be taken into great consideration. During the transmission phase, such data can be extremely sensitive and therefore need to

be secured from all adversaries that can intercept them. Several security solution methods have been developed in the past to securely hide data. Most of the commonly adopted security approaches are based on cryptography, steganography (Karaman and Sagiroglu, 2012), modified steganography and their hybrid versions (Osunade and Ganiyu, 2016).

The solutions based on steganography approaches have shown to completely hide the existence of the secret data (Nashat and Mamdouh, 2019) thereby giving attackers little or no opportunity to suspect its existence (Kradi and Pal, 2014). Steganographic algorithms can exist in both spatial and transform domains (Falesh *et al.*, 2014; Farah and Alyousuf, 2020). The first and most widely accepted method in the spatial domain is the Least Significant Bit (LSB) (Aini, 2019), which is due to its simplicity of execution (Caldwell, 2003), high embedding

capacity and low computational complexity (Syed *et al.*, 2018).

Furthermore, some of the most currently existing improvements on LSB include LSB based on selective and randomized approach (Younes and Jantan, 2008), LSB with Sample Pairs Analysis (Roque and Minguet, 2009), Fingerprint biometric with LSB, 3-DWT and RSA (Mayank *et al.*, 2015). Improving LSB with Pseudo Random Number Generator (Nadia, 2016), chaos-based logistic map with LSB (Özcan and Kemal, 2017) encryption RSA-LSB (Apau and Adomako, 2017), Linear Congruential Generator (LCG) for insertion of data in LSB (Rajput & Ramesh, 2018), LSB with integer wavelet transform (Elshazly *et al.*, 2018), Inserting secret message in the blue section of an image using LSB and RSA (Riza *et al.*, 2019), Adaptive Genetic Algorithm (AGA) support for LSB embedding process (Denis & Madhubala, 2020), Modification of LSB using bit inverse insertion and the length of the text (Fahrul *et al.*, 2021), Hybrid nLSB method of image steganography within spatial plane (Kemal & Özcan, 2021), Compressed text and images with LSB (Osama *et al.*, 2021) and so on. In most cases, these improvements only have supports for cover images in BMP, PNG and TIFF image formats.

They often produce high imperceptibility and transparency with cover images in JPEG format. In the same vein, most of these approaches are highly complex and often computational resource intensive. As a result, major improvements to these security algorithms are required.

LITERATURE REVIEW

Data Security Techniques

In recent times, the security of information has been one of the most important issues in Information and Communication Technology (ICT) due to the upsurge in the use of the internet in the past decade (Pandikumar and Tesfay, 2016). The increased use of

computers and development of computing technology in all spheres of life has placed information security at the front burner of computing research, a major concern being the concept of hiding sensitive information during transmission or information exchange (Deepa, 2015). The internet provides a means of communication and distribution of information and this has increased the use of different methods of hiding information in various multimedia (Provos and Honeyman, 2003).

Data security can be defined as efforts put in place to prevent unauthorized individuals from gaining access, corrupting, or stealing digital information throughout its complete lifecycle. It is a term that combines all levels of security, from physically securing hardware and storage devices to organizational policies and procedures, access controls, and the security of all software applications (IBM, 2021). It includes all processes and practices adopted to safeguard Information Technology (IT) environment from unwanted internal or external influence (Harrington, 2021) and one of the most important factors in any business organization (Marsaid, 2020). Today, the most cost effective and widely adopted way of exchanging large volume of highly confidential information without boundaries is over the internet (Prachi, 2017). More often than ever before, the rate at which the internet is used for the daily transmission of sensitive digital information and data calls for the continuous research and development of new ways and technologies for data security (Chen, 2018).

Cryptography

Since time immemorial, humans have always had the natural need to selectively communicate and share information. These needs gave way to the art of using different means and methods in securing messages sent from one point to another so that only authorized recipients can have access to them. With this, third parties find it difficult to excerpt any information

from the encrypted message even if the cipher text falls in their hands.

The word cryptography comes from the two Greek words “kryptos” meaning hidden and “gràphein” meaning writing, thus the word cryptography means hidden writing (Babu *et al.*, 2013; Oppliger, 2016; Marwa *et al.*, 2016). Cryptography has been defined by several researchers as the practice and study of procedures used to guarantee information security during communication or data transmission between authorized parties and preventing unauthorized access to the information being transmitted, the procedure includes encryption and decryption. While Phil Zimmermann defined it as the application of mathematical science to encrypt and decrypt data, it has been defined as the art and science of ensuring the security of messages (Adomey, 2021).

Related works

Deepesh and Vijaya (2013) proposed an improvement on LSB for hiding secret messages in color images. This was done by substituting each character in a text file, including special characters and embedding each bit of every character in the Last Significant Bit of the cover image’s pixel respectively. The peak signal to noise ratio (PSNR) from evaluation was very high while the Mean Squared Error (MSE) was low, showing good stego quality. They however did not present an additional layer of security such as cryptography and more metrics for evaluation in order to validate the strength of the improvement. Arun *et al.* (2015) provided the process involved in concealing text in images using (LSB). The embedding space, maintaining secrecy of texts, adopted key distribution technique were major limitations of this study. They could only hide texts that are equal to the size of messages and additional layer of security using cryptography.

Mohammed and Rossilawati (2015) discussed an improvement on LSB based steganography by bit

inversion method to enhance the quality of 24-bit stego-images. The modifications performed are quite good, they nevertheless have limited capability positioning pixels in cover-image (Fahrul *et al.*, 2021). Varsha and Rajender (2015) developed an algorithm using an improved LSB coding technique and encryption with RSA, confidential text was embedded in an image file. The binary equivalents of both files were converted and embedding process was made more robust by using XOR function.

Rachmawanto (2020) analyzed the use of RSA to encrypt the LSB of RGB color images in three patterns of information hiding. Using the same dataset for the cover image and message to be sent, the patterns were compiled by a third method. Before embedding the message, it was encrypted using RSA making process develop issues with payload and imperceptibility. Denis and Madhubala (2020) designed a unique hybrid cryptosystem, using both RSA and AES algorithms to secure private messages hidden in a cover image. They also enhanced the embedding capacity of LSB by applying a novel Adaptive Generic Algorithm (AGA); the resultant cryptosystem is however heavyweight and the authors suggested the design of a lightweight cryptosystem which offer same or better security features for data transmission.

Pramanik and Ramkrishna (2020) proposed a system that conceals data using cryptography and steganography, taking into account two factors: the size of the object to be encrypted and the minimum level of security required. Message authentication/integrity and non-repudiation are all possible with their system but requires continuous support to increase its potential for better message authentication. Khan (2020) made attempt to conceal any trace of information by masking encrypted data under the cover of steganography. LSB steganography was implemented by introducing uncertainties while embedding the bits which helps

disconnect the repeated replacement of secret message. They successfully implemented a reliable steganography system which permits the reusability of the cover-image, an advantage over prevailing techniques in which the original image must be kept secret until it is accessed by the intended recipient. The results from the test conducted on the proposed system does not totally guarantee transparency and imperceptibility, they also suggest tough resistance to LSB Steg-analysis procedures.

Based on the results of the related works reviewed, one could infer that both steganography and cryptography methods are individually insufficient for the required level of security for information in all scenarios; evaluations were also insufficiently carried out.

Most of the developed crypto-steganographic methods do not perform well when the cover image used is in JPEG and BMP formats or if the size of the secret data is substantial, they require a lot of processing time and computational resources. The proposed methodology will address these challenges in the existing crypto steganographic methods and evaluate the performance using at least five metrics.

RESEARCH METHODOLOGY

Research Approach

In this research, an improved crypto-steganographic algorithm based on the combination of a modified LSB algorithm (RSA-LSB-DWT) to secure data transmission via digital images was developed. The implementation of the developed modified crypto-steganographic algorithm is made up of three distinct stages which include:

- i. Cover Image Dataset acquisition.
- ii. Introduction of CoverImage to the RSA-LSB-DWT Algorithm for secret data hiding.
- iii. Design and implementation of the proposed crypto-steganographic algorithm.

Cover Image Dataset Acquisition

Image dataset acquired for the purpose of this research are in JPEG, BMP, PNG and TIFF formats, which are passed into the developed algorithm for processing and evaluation. The encryption and decryption algorithm adopted was RSA (Rivest–Shamir–Adleman), while the embedding process (mLSB+DWT) was achieved by modifying the LSB (Least Significant Bit) with the application of DWT (Discrete Wavelet Transform). The encryption of the plain text preceded the encompassed image compression, modification, quantization and determination of the correct sub-bands was needed to decrease execution time. The results obtained were evaluated using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Image Fidelity, Normalized Cross Correlation Embedding Rate and Average Difference to determine the performance of the developed techniques. Figure 3.1 illustrates the scheme of this study.

Image Acquisition and Processing

The image files for this research were acquired online via [ImageProcessingPlace \(https://www.imgonline.com.ua/eng/\)](https://www.imgonline.com.ua/eng/), which provides access to several standard digital test images often found in literatures including Lena, Baboon, and pepper etc., in uncompressed formats and same size (512 x 512) in JPEG, BMP, PNG and TIFF which are popular image formats, have the same resolution and high definition. Table 3.1 shows the properties of image formats used and describes the processing operations performed on the acquired images.

The proposed algorithm is divided into three phases, i.e. the key generation phase, the stegosystem embedding phase and the stegosystem extraction phase. Each phase is discussed in details as follows:

The key generation phase is the first and a very important step requisite for the RSA algorithm, and

is used to generate the public and private keys required for the encryption and decryption of the plain text.

Table 3.1: Properties of image formats used

Image Format	Image Name	Size (Kb)	Width (pixels)	Height (pixels)
JPEG	Lena	75	515	515
	Baboon	141	515	515
	Airplane	72	515	515
	Pepper	87	515	515
BMP	Lena	768	515	515
	Baboon	768	515	515
	Airplane	768	515	515
PNG	Pepper	768	515	515
TIFF	Lena	404	515	515
	Baboon	602	515	515
	Airplane	353	515	515
	Pepper	458	515	515
	Lena	774	515	515
	Baboon	774	515	515
	Airplane	773	515	515
	Pepper	774	515	515

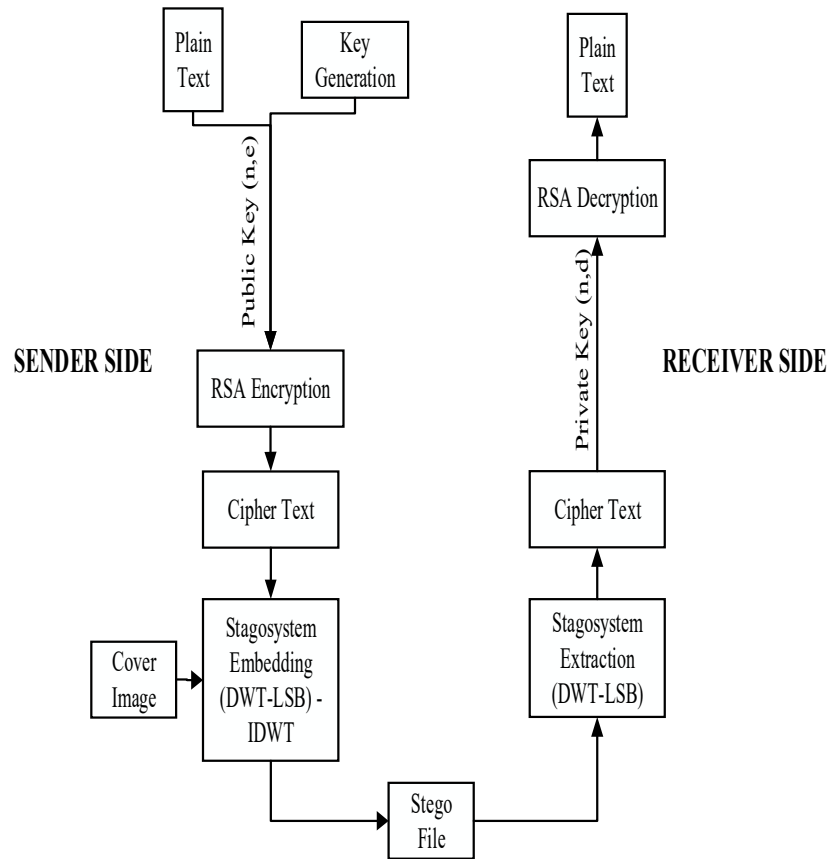


Figure 3.1: Block Diagram of the Proposed Modified LSB with RSA

This phase serves as the entry and exit points of the proposed algorithm. It brings in key complexity for the encryption process required to convert the plain text into cipher-text and also offers a comparable level of complexity for the decryption process. The algorithm is stated below.

Stegosystem Embedding Phase (DWT-LSB)

This phase is divided into two steps, i.e. encrypting the plain text using RSA encryption technique and embedding data in image using a modified LSB Encoding System. The details of each step are outlined in the next Algorithm 3.2:

Algorithm 3.1 RSA Key Generation

RSA_Keygen()

INPUT:
Two large prime numbers p and q .

OUTPUT:
Public Key Components: $\{e, n\}$ where e is the public key and n is the block size
Private Key Components: $\{d, n\}$ where d is the private key and n is the block size.

PROCEDURE:
 $n \leftarrow p * q$
/ Compute Euler Phi value of n */*
 $\Phi(n) \leftarrow (p - 1) * (q - 1)$
 Find a random number e , satisfying $1 < e < \Phi(n)$ and $\text{gcd}(e, \Phi(n)) = 1$.
 Compute a random number d , such that,
 $d \leftarrow e^{-1} \text{ mod}(\Phi(n))$

Algorithm 3.2: RSA encryption and data embedding using developed LSB-DWT Encoding Algorithm

STEP 1: Encrypt message using the RSA Encryption Algorithm

RSA_Encrypt ()

INPUT:
Plain Text Message, $M (< n)$

OUTPUT:
Cipher Text, C

PROCEDURE:

- i. Receiver sends a message or plaintext $M (< n)$ along with public keys to Sender
- ii. Sender encrypts the message using Receiver's public key e to generate Cipher Text, C

$\text{Cipher Text, } C \leftarrow M^e \text{ mod } n$

STEP 2: Embed data in image using Modified LSB-DWT Encoding Algorithm

Message_Embed ()

INPUT:
Cipher Text, C

OUTPUT:
Stego Image

PROCEDURE:

- i. Read the cover image.
- ii. Apply DWT on the cover image
- iii. Convert the RGB image into a vector of 0s and 1s and message to their respective binary forms.
- iv. Compare image size with message bits.
- v. This vector P is again divided into n parts. Three bits of the message is hidden in the least significant bit (LSB) of each blue pixel of the image which are then embedded into the corresponding LL and HH sub bands. The stego pixels is embedded with strength x into the maximum coefficient M_j of each image block Y_j
The embedding equation is:

$$Y_j = M_j + \frac{C_j}{M_j} * x$$

- vi. Continue procedure until all message is fully hidden in cover image.
- vii. The stego luminance element of the image is obtained using inverse DWT. Lastly, stego file is reconstructed and stego image obtained.

Algorithm and the decryption process using the private key detailed in Algorithm 3.1.

Stegosystem Extraction Phase (DWT-LSB)

This consists of two steps, i.e. to retrieve data from the image with the modified LSB Decoding

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)

PSNR expresses the ratio between the maximum potential value of the power of noise distortion and

signal in relation to its effects on the quality of image representation (Khan, 2020). This ratio is very useful in measuring the quality between original and resultant images. Given that the ratio between the biggest and lowest possible values of a variable quantity is quite large, PSNR is typically expressed in the form of a logarithmic decibel (dB) and can be used to measure test qualities performed on images. The higher the PSNR value of an image the better its quality, the confidentiality of an image is preserved if the set dB is greater than the PSNR.

Given two streams stored in vectors X and Y, the Mean Squared Error (MSE) is calculated as follows:

$$MSE = \frac{1}{n} \sum_{i=1}^n (X[i] - Y[i])^2 \quad 3.3$$

Given that streams X and Y stated above is the original image and its encryption, then the PSNR can be calculated as:

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad 3.4$$

Where MAX = maximum potential value of the image's pixel

MSE allows for the easy identification of the differences between the pixel values of the original image and resultant image. It is a representation of the average squares of errors between the original and enhanced images. The error signifies the difference in value, between the original and enhanced images. A higher MSE suggests a great difference between the original and enhanced images, thus a higher error and vice versa.

Image Fidelity

This is concerned with checking if an image enhancing process can produce an image more accurately, free of any noticeable distortion/information loss, very useful in measuring

the closeness of an enhanced image to the ideal image. It uses visual information of an image to measure any relative distorted digital image information with reference to the original image. It can be used to predict quality enhancement because of contrast improvement

If the difference between the original and resultant images cannot be detected, then it can be concluded that an image enhancing process is visually lossless (Adomey, 2021). It is quite feasible to develop calculative estimates of image fidelity grounded on human vision mockups since these categories of conclusions largely rely on how we can detect the visual differences between an original and resultant image. Image fidelity was used to test the robustness of the proposed algorithm; fidelity measures calculated by image fidelity can be computed using the following equation.

$$Image\ Fidelity = 1 + \frac{\sum_{i,j} (P(i,j) - S(i,j))^2}{\sum_{i,j} (P(i,j) \times S(i,j))} \quad 3.5$$

P(i, j) = the value of the pixel at ith row and jth column
S is the number of bits

(i, j) = the respective indices of row and column numbers.

Alternatively,

$$Image\ Fidelity = 1 - \frac{\sum_{i=1}^M \sum_{j=1}^N (x(i,j) - y(i,j))^2}{\sum_{i=1}^M \sum_{j=1}^N x(i,j)} \quad 3.6$$

Where:

M = Quantity of horizontal pixels

N = Quantity of vertical pixels

x(i, j) = filtered image at i and j axis

y(i, j) = noisy image at i and j axis

Normalized Cross Correlation (NCC)

This is a commonly adopted metric in digital image processing to appraise the degree of resemblance between an original and resultant image (Prachi,

2017). To get the incidence of a digital image's pattern, it can be first normalized when its brightness varies due to lightning exposure and other variables. It is useful in image registration and assessment of quality resampling procedures. When compared to Ordinary Cross Correlation (ORD), NCC has minimal sensitivity to linear variations in the generosity of illumination, and values are restricted between -1 & 1 (-1 specifies impeccable correlation while 1 specifies flawless anti-correlation). NCC does not have limited frequency domain expression with simpler setting for threshold value.

A normalized correlation between two images can be defined as:

$$\frac{\sum_{i=1}^M \sum_{j=1}^N (x(i,j) - y(i,j))^2}{\sum_{i=1}^M \sum_{j=1}^N x(i,j)} \quad 3.7$$

Where:

M = Quantity of horizontal pixels

N = Quantity of vertical pixels

$x(i, j)$ = filtered image at i and j axis

$y(i, j)$ = noisy image at i and j axis

Image histogram

This can be used to test how strong a steganographic image is to guide against statistical attacks, when the host image has the same color as the histogram of the resultant image (Marsaid, 2020). In digital images, it provides histograms (of graphical representation) that are used as tonal distribution. A visual inspection of the histogram of a particular image will easily give away the tonal distribution because they are plotted using the number of pixels of each tonal value, thus one can easily tell the difference in an original and resultant image. Statistical security analysis includes Entropy, Correlation, Homogeneity, Contrast and energy.

Average Difference

This is the pixel difference between an enhanced and corresponding disintegrated image. It is a measurable quantity used for exclusive object detection and

applicable to all image processing applications that requires getting the variance between two images (Marsaid, 2020). The larger the Average Difference value, the poorer the quality of an image.

$$\frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (x(i,j) - y(i,j)) \quad 3.8$$

M = Quantity of horizontal pixels

N = Quantity of vertical pixels

$x(i, j)$ = filtered image at i and j axis

$y(i, j)$ = noisy image at i and j axis

RESULTS AND DISCUSSION

Results

This chapter discusses the results of the traditional Least Significant Bits (LSB) with Rivest Shamir Adleman algorithm (RSA) and the modified LSB (mLSB) with Discrete Wavelength Transform (DWT) and RSA. The results of the developed algorithm were also compared with existing state of the art algorithms. A graphical user interface with three frames for sender, unsecure transmission channel and receiver was developed using MATLAB 2020a to perform operations and obtain results from the algorithms. As shown in Figure 4.1a, the sender frame consists of a text field to type the message to be encrypted. It also displays the message in plain text and presents the desired cover image to embed the message on. The unsecure transmission frame consists of eight command buttons and is where all the operations are performed. The buttons are for loading the desired cover image, encrypt and embed, extract and decrypt, embed, decrypt, clear the result table, display results and save/export results. It also has two check buttons for selecting the desired technique, i.e. RSA-DWT-LSB and RSA-LSB and displays the encrypted text. The receiver frame presents the decrypted message and the stego image. After the application is launched, the sender types the message to be encrypted in the space provided and selects a cover image using the "Load Image" button.

Clicking the “Encrypt and Embed” button automatically encrypts the message, displays it in the space provided and then embeds it on the cover image. The corresponding stegoimage is generated and displayed at the receiver’s end. To retrieve the cover image, the receiver clicks on the “Extract and Decrypt” button.

The time taken to encrypt and decrypt in RSA-DWT-LSB and RSA-LSB techniques were utilized to evaluate the results of each image format. In addition, the MSE, RMSE, PSNR, NCC, and Image Fidelity were used to assess the techniques.

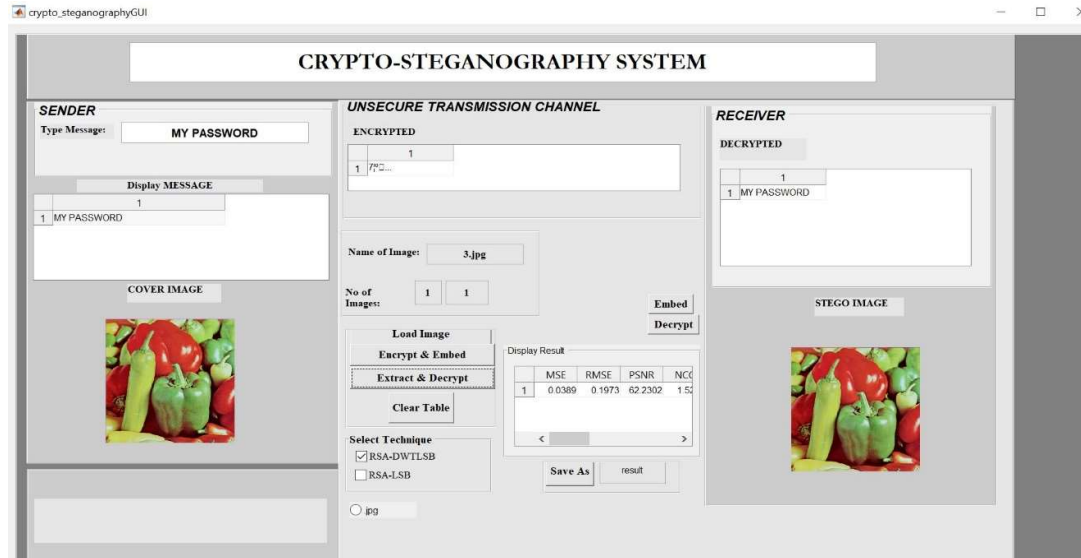
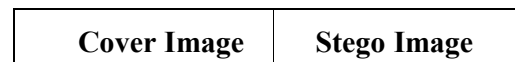


Figure 4.1a Implementation menu of the developed RSA-mLSB+DWT Crypto-Steganography Technique.

Result of Encryption and Decryption Times for RSA-LSB and RSA-mLSB+DWT Techniques

Tables 4.1a and b presents the encryption and decryption times used in determining the pace of encrypting and decrypting standard images i.e. Airplane, Baboon, Pepper and Lena for both techniques. Using BMP format, RSA-mLSB+DWT technique took 5.896ms, 4.949ms, 5.595ms and 4.959ms to encrypt and embed the message on the images respectively, while the decryption time was 4.399ms, 4.701ms, 4.783ms and 4.386ms. However, RSA-LSB took 10.705ms, 10.392ms, 11.338ms and 10.268ms to perform encrypt and embed operation, and 11.580ms, 11.940ms, 13.117ms and 11.199ms for decryption. For PNG, it took RSA-mLSB+DWT 4.959ms, 5.427ms, 5.596ms and

5.308ms respectively to encrypt and embed the text on the images, and 4.715ms, 4.476ms, 4.730ms and 4.838ms decryption time while RSA-LSB used 11.984ms, 11.676ms, 12.617ms and 10.045ms for encrypt and embed, and 10.616ms, 9.032ms, 11.053ms and 9.191ms for decryption. With RSA-mLSB+DWT, the TIFF format required 4.984ms, 4.917ms, 5.638ms and 5.839ms respectively for encrypt and embed process and 4.664ms, 4.209ms, 4.157ms and 4.371ms decryption time whereas it took RSA-LSB 10.714ms, 9.607ms, 11.980ms and 9.818ms to encrypt and embed, and 9.551ms, 9.297ms, 10.261ms and 9.069ms decryption time on the same set of images.





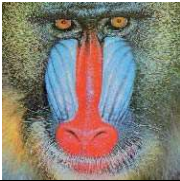
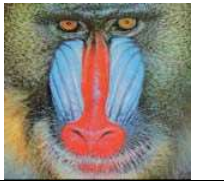




	
Lena	mLSB+DWT
	
Baboon	mLSB+DWT
	
Pepper	mLSB+DWT
	
Airplane	mLSB+DWT

Figure 4.1b: Visual Comparison of Cover and Stego images

Lastly, for the JPEG format, it took RSA-mLSB+DWT 5.318ms, 5.549ms, 5.503ms and 5.3894ms.1449ms, and 4.1449ms, 4.7588ms 4.7405ms and 4.6209ms decryption time, while it took RSA-LSB 12.619ms, 11.546ms, 10.538ms and 9.816ms respectively to encrypt and embed the images, and 11.694ms, 9.586ms, 9.004ms, 9.392ms for decryption.

Table 4.1: Encryption and Decryption Time using distinct image formats for RSA-mLSB+DWT and RSA-LSB

(a) Encryption Time

In all cases and formats, the developed algorithm had better embed and encrypt, and decryption time as presented in table 4a and b.

The shorter the encryption/decryption time, the better the algorithm’s performance (Mittal&Kansal, 2014). From tables 4.1a and 4.1b, it is quite obvious that the developed algorithm out performs RSA-LSB in terms of encryption and decryption time. The time required for encrypting JPEG image format is less than the time required for encrypting all other formats which is a major concern in exiting techniques as most do not perform well with JPEG file format.

Results of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Root Mean Square Error (RMSE) for RSA-mLSB+DWT and RSA-LSB Techniques

Tables 4.2a, b, c presents the PSNR, MSE, and RMSE results of the different image formats using the RSA-mLSB+DWT and RSA-LSB techniques. Centered on these results, it was discovered that both the RSA-mLSB+DWT technique outperformed RSA-LSB.

Using the RSA-mLSB+DWT technique, the PSNR values obtained for the BMP standard images (Airplane, Baboon, Pepper and Lena) are 72.06dB, 65.089dB, 62.23dB and 67.03dB respectively. For PNG image format, the values were 70.01dB, 65.08dB, 62.49dB and 67.03dB respectively and the corresponding values for TIFF image format were 70.98dB, 65.08dB, 62.23dB and 68.48dB while that of JPEG was 73.29dB, 65.09dB, 62.49dB and 67.03dB respectively. Similarly, with the RSA-LSB technique, the PSNR values obtained for the BMP standard images are 58.89dB, 59.76dB, 58.16dB and 59.76dB respectively.

Image Format	Image Name	Size (Kb)	RSA-mLSB+DWT (ms)	RSA-LSB (ms)
JPEG	Airplane	72	5.318	12.619
	Baboon	141	5.549	11.546
	Pepper	87	5.503	10.538
	Lena	75	5.389	9.816
BMP	Airplane	768	5.896	10.705 10.392
	Baboon	768	4.949	11.338 10.268
	Pepper	768	5.594	
	Lena	768	4.959	11.984
PNG	Airplane	353		11.676
	Baboon	602	4.9595.4275.596	12.617
	Pepper	458	5.308	10.044
	Lena	404		
TIFF	Airplane	773	4.984 4.917	10.7149.607
	Baboon	774	5.638 5.839	11.980 9.818
	Pepper	774		
	Lena	774		

(b) Decryption Time

Image Format	Image Name	Size (Kb)	RSA-mLSB+DWT (ms)	RSA-LSB (ms)
JPEG	Airplane	72	4.145	11.6949.586
	Baboon	141	4.7594.740	9.004
	Pepper	87	4.621	9.392
	Lena	75		
BMP	Airplane	768	4.398 4.701	11.580
	Baboon	768	4.7834.386	11.940
	Pepper	768		13.117
	Lena	768	4.7154.4764.730	11.199
PNG	Airplane	353		10.6169.032
	Baboon	602	4.664 4.209	11.053 9.191
	Pepper	458	4.157 4.371	
	Lena	404		9.551
TIFF	Airplane	773		9.297 10.261
	Baboon	774		9.069
	Pepper	774		
	Lena	774		

For PNG image format, the values were 58.69dB, 59.31dB, 59.09dB and 59.76dB respectively and the corresponding values for TIFF image format were 58.89dB, 59.76dB, 59.76dB and 59.76dB while that of JPEG was 59.53dB, 60.28dB, 58.17dB and 58.17dB respectively.

The results for MSE using RSA-mLSB+DWT on standard images (Airplane, Baboon, Pepper and Lena) in BMP format are 0.004dB, 0.020dB, 0.039dB and 0.013dB respectively. PNG produced 0.006dB, 0.020dB, 0.037dB and 0.013dB while the values for TIFF are 0.005dB, 0.020dB, 0.039dB and

0.009 respectively. Lastly, the values obtained for the JPEG format are 0.003dB, 0.020dB, 0.037dB and 0.013dB. The corresponding values using RSA-LSB technique are 0.084dB, 0.069dB, 0.099dB, 0.069dB respectively for BMP format while PNG generated 0.088dB, 0.076dB, 0.080dB and 0.069dB values respectively. The values for TIFF format are 0.084dB, 0.069dB, 0.088dB and 0.069dB, finally the values obtained for the JPEG format are 0.072dB, 0.061dB, 0.099dB and 0.084dB respectively.

Furthermore, Table 4.2c present results for the RMSE using RSA-mLSB+DWT on standard images (Airplane, Baboon, Pepper and Lena) in BMP format

are 0.06dB, 0.14dB, 0.19dB and 0.11dB, PNG obtained values of 0.08dB, 0.14dB, 0.19dB and 0.11dB respectively while the values for TIFF are 0.07dB, 0.14dB, 0.19dB and 0.09db. Lastly, the values using JPEG format are 0.06dB, 0.14dB, 0.19dB and 0.11dB. The corresponding values using RSA-LSB technique are 0.28dB, 0.26dB, 0.31dB and 0.26dB respectively for BMP format while PNG generated 0.29dB, 0.27dB, 0.28dB and 0.26dB values respectively. The values for TIFF format are 0.28dB, 0.26dB, 0.29dB and 0.26dB, finally the values obtained for the JPEG format are 0.27dB, 0.24dB, 0.31dB and 0.29dB respectively.

Table 4.2: PSNR, MSE, and RMSE using different images formats for RSA-mLSB+DWT and RSA-LSB Techniques

(a) Peak Signal to Noise Ratio (PSNR)

Image Format	Image Name	Size (Kb)	RSA-mLSB+DWT (dB)	RSA-LSB (dB)
JPEG	Airplane	72	73.285	59.537
	Baboon	141	65.089	60.275
	Pepper	87	62.494	58.166
	Lena	75	67.027	58.892
BMP	Airplane	768	72.063	58.892
	Baboon	768	65.089	59.763
	Pepper	768	62.230	58.166
	Lena	768	67.027	59.763
PNG	Airplane	353	70.012	58.699
	Baboon	602	65.089	59.306
	Pepper	458	62.494	59.094
	Lena	404	67.027	59.763
TIFF	Airplane	773	70.981	58.892
	Baboon	774	65.089	59.763
	Pepper	774	62.230	58.699
	Lena	774	68.478	59.763

(b) Mean Square Error (MSE)

Image Format	Image Name	Size (Kb)	RSA-mLSB+DWT	RSA-LSB (dB)
--------------	------------	-----------	--------------	--------------

			(dB)	
JPEG	Airplane	72	0.003	0.072
	Baboon	141	0.020	0.061
	Pepper	87	0.037	0.099
	Lena	75	0.013	0.084
BMP	Airplane	768	0.004	0.084
	Baboon	768	0.020	0.069
	Pepper	768	0.039	0.099
	Lena	768	0.013	0.069
PNG	Airplane	353		
	Baboon	602	0.006	0.088
	Pepper	458	0.020	0.076
	Lena	404	0.037	0.080
TIFF	Airplane	773	0.013	0.069
	Baboon	774		
	Pepper	774	0.005	0.084
	Lena	774	0.020	0.069
			0.039	0.088
			0.009	0.069

(c) Root Mean Square Error (RMSE)

Image Format	Image Name	Size (Kb)	RSA-mLSB+DWT (dB)	RSA-LSB (dB)
JPEG	Airplane	72	0.055	0.269
	Baboon	141	0.142	0.247
	Pepper	87	0.191	0.315
	Lena	75	0.114	0.289
BMP	Airplane	768	0.064	0.289
	Baboon	768	0.141	0.262
	Pepper	768	0.197	0.315
	Lena	768	0.114	0.262
PNG	Airplane	353		
	Baboon	602	0.080	0.296
	Pepper	458	0.142	0.276
	Lena	404	0.191	0.283
TIFF	Airplane	773	0.113	0.262
	Baboon	774		
	Pepper	774	0.072	0.289
	Lena	774	0.142	0.262
			0.197	0.296
			0.096	0.262

Based on PSNR, MSE and RMSE, the results presented confirmed that RSA-mLSB+DWT outperformed RSA-LSB using various image formats

which demonstrates improved robustness over prevailing methods as well as improved quality and reduced error.

The time taken to encrypt and decrypt in the developed encryption technique (RSA-LSB+DWT) evaluated revealed that the modification of LSB in conjunction with DWT resulted in a decrease in encryption and decryption time as shown in Tables 4.1 for all image formats (JPEG, BMP, PNG and TIFF) used in this research. The results from this table captures the improvement between the two techniques, in all cases RSA-mLSB+DWT had better encryption and decryption time. The smallest

encryption time value of 4.4ms was obtained from Lena in JPEG format while the highest was obtained from Airplane with 7.4ms in PNG format, this also validates the better performance of the developed algorithm. The introduction of the fast compression capability of DWT facilitated the overall reduction time of the algorithm, this helped in decreasing the computational overhead associated with LSB when working on complex multimedia images (Kalpana and Mangal, 2016). Figure 4.2 shows the performance graph of techniques in relation to encryption and decryption time.

Bbbbbbbbbbbb

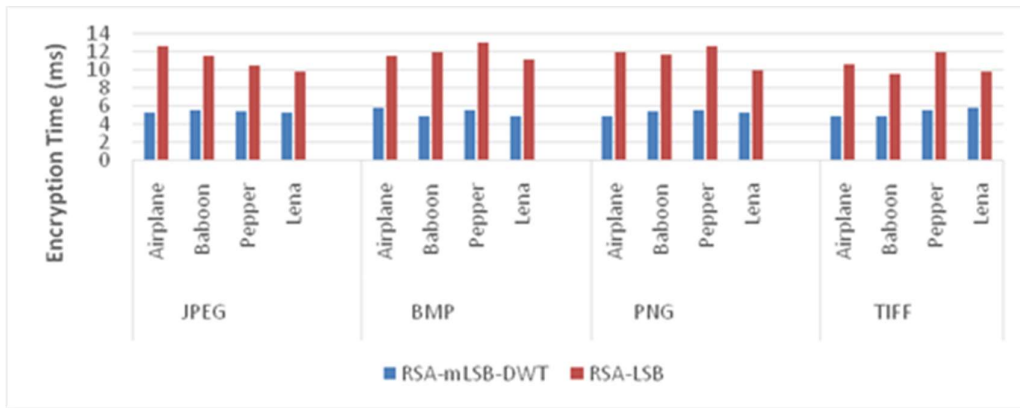


Figure 4.2: Encryption Time for image formats with RSA-mLSB+DWT and RSA-LSB

Comparison with other state-of-the-art methods

There have been several modifications to LSB but this research work is similar to those of (Prabakaran&Bhavani, 2012; Jueja& Sandhu, 2013; Elshazlyet al. 2016; Elshazlyet al. 2018 and Swati & Manish, 2019). Table 4.4 present results of these methods for easy comparison with that of the developed method in Table 4.5 using BMP format. Majority of the methods presented gave promising performance, the developed technique however gave an outstanding performance in relation to PSNR, MSE. The result presented in Tables 4.5 shows that the developed technique has the best performance among the list and confirms that the technique

performs well when matched with existing and other conventional methods based on performance.

CONCLUSION AND RECOMMENDATION

The essential features of a modified LSB Cryptosteganographic security of digital images were evaluated, to achieve this, online uncompressed image files in in JPEG, BMP, TIFF and PNG formats were obtained from a reliable online repository. The concept of security in image steganography was discoursed and a mechanism that provides improvement in the security of hidden data using modified LSB and DWT was developed.

Table 4.4: Evaluation results from similar methods

Color image (512×512)	LSB			DWT-LSB			IWT-LSB		
	MSE	PSNR	NCC	MSE	PSNR	NCC	MSE	PSNR	NCC
Lena	0.18	55.49	1.00	0.18	55.56	1.00	0.18	55.52	1.00
Baboon	0.18	55.54	1.00	0.18	55.55	1.00	0.18	55.56	1.00
Pepper	0.17	55.18	1.00	0.18	55.18	1.00	0.17	55.20	1.00
Airplane	0.18	54.84	1.00	0.18	54.80	1.00	0.18	54.80	1.00

Table 4.5: Evaluation results from developed technique

Color Image (512 X 512)	mLSB+DWT		
	MSE	PSNR	NCC
Lena	0.013	67.027	0.506
Baboon	0.20	65.089	0.790
Pepper	0.39	62.230	0.526
Airplane	0.004	72.063	0.159

The developed technique, mLSB+DWT was adopted to successfully hide and retrieve information on standard digital images. The study aimed at developing an improved LSB technique by overcoming the standard LSB technique's high imperceptibility and transparency, especially in JPEG and BMP formats which are sought-after characteristics of a truly secure and reliable security technique for remote data transmission.

The standard LSB was modified to create a balance between the algorithm's exploration and exploitation stages so as to improve quantity solution in detecting high energy coefficient (optimal wavelet coefficient) of DWT and to resolve conflicting requirements of different parameters and properties of digital images. The techniques achieved improved Average difference, MSE, RMSE, PSNR, Image Fidelity and NCC, indicating a higher quality measurement between the original and compressed images using different formats.

The results from simulations proved that the developed algorithm guaranteed good imperceptibility while maintaining perceptual quality. The results of the evaluation presented show significant improvements in relation to robustness transparency and imperceptibility which justifies that using modified LSB in combination with DWT for securing information as a more effective way to enhance the performance of the popular traditional LSB algorithm security.

In relation to the performance of the developed techniques, the mLSB+DWT encryption technique can be applied to deal with the challenges associated with the standard LSB algorithm during the transmission of sensitive information and guarantee the secrecy and protection of data. Since the techniques for image crypto-steganography and other application areas is ongoing research, the following recommendations are made for future study:

- i. For possible performance enhancement, the improved LSB should be combined with other DWT variants such as Bi-orthogonal Wavelet Transform, 2D-DWT, and other watermarking algorithms.
- ii. An alteration of the fitness function of evolutionary search algorithm with high convergence speed and accuracy, such as Particle Swarm Optimization (PSO), Cat Swarm Optimization (CSO) and Firefly

Algorithm (FA), can be applied to locate the high energy coefficient in DWT.

- iii. The patent is applicable to hardware implementation on Integrated Circuits (IC) and could be tried on other platforms.

This work is expected to contribute to knowledge by:

1. The creation of a modified LSB (mLSB+DWT) algorithm combined with RSA to enhance secured data transmission and dealing with computational overhead associated with traditional LSB.
2. Exemplified the use of high energy coefficient in DWT for improved image security, robustness and quality.
3. Reduction of imperceptibility and transparency of stego-images by removal of visible degradation on cover images during remote data transmission.
4. Extensive performance evaluation report on the developed algorithm across several standard evaluation metrics using the same dataset.

Declaration of Competing Interest

This is to certify that this research work did not receive any funding and there is no competing interest.

REFERENCES

Amir, D. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Science*, 11, 4580 <https://doi.org/10.3390/app11104580>.

Apau, R., and Adomako, C. (2017). Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones. *International Journal on Computer Applications*, 164(1):13-22 13-22.

Karaman, H. B., and Sagiroglu, S. (2012). An Application Based on Steganography. *ASONAM*

'12: *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)USA: IEEE Computer Society*, August 2012, 839–843 <https://doi.org/10.1109/ASONAM.2012.152>.

Osunade, O., and Ganiyu, I. A. (2016). Enhancing the Least Significant Bit (LSB) Algorithm for Steganography. *International Journal of Computer Applications*, 149(3):1-8.

Nashat, D., & Mamdouh, L. (2019). An efficient steganographic technique. *Journal of the Egyptian Mathematical Society*, 1-4.

Krati, Vyas., and Pal, B. L. (2014). A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique. *International Journal of Advanced Research in Computer and Communication Engineering*, 3(4): 5246-5251.

Falesh, M. S., Ashwini, A. D., and Pravin, D. S. (2014). Comparison of different techniques for Steganography in images. *International Journal of Application or Innovation in Engineering & Management (IJAIEEM)*, 3(2):171-175.

Farah, Q. A., and Alyousuf, R. D. (2020). Analysis review on spatial and transform domain technique in digital steganography. *Bulletin of Electrical Engineering and Informatics*, 9(2):573-581.

Aini, D. R. (2019). Survey of Methods in the Spatial Domain Image Steganography based Imperceptibility and Payload Capacity. *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 4(2):434-439.

Caldwell, J. (2003). Steganography. *CROSSTALK. The Journal of Defense Software Engineering*, 25-27.

- Syed, M. H., Salihah, Y., Syed, B., Mehvish, S., & Zahid, G. K. (2018). Comparison of LSB And DWT Steganography Techniques. *International Journal of Advance Engineering and Research*, 24(1):1-5.
- Younes, M. A. J. (2008). Image Encryption Using Block-Based Transformation Algorithm. Corpus ID: 16397291.
- Roque, J. J., and Minguet. (2009). SLSB: Improving the Steganographic Algorithm LSB. *Security in Information Systems, Proceedings of the 7th International Workshop on Security in Information Systems, WOSIS 2009, In conjunction with ICEIS 2009, May 2009. Milan, Italy.: ICEIS.*
- Mayank, G., Shashikant, G., and Pallavi, K. (2015). Fingerprint Watermarking and Steganography for ATM Transaction using LSB-RSA and 3-DWT Algorithm. *International Conference on Communication Networks (ICCN)*, 1(1): 246-251.
- Özcan, C., and Kemal, T. (2017). Improvement Of LSB Based Image Steganography. *Proceedings of Research World International Conference*, (pp. 36-40). Rome, Italy.
- Nadia, M. (2016). Increasing Security In Steganography By Combining LSB and PRGN. *International Journal of Computer Science and Mobile Computing*, 5(2):34-38.
- Apau, R., and Adomako, C. (2017). Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones. *International Journal on Computer Applications*, 164(1):13-22.
- Rajput, G., and Ramesh, C. (2018). Improved Lsb Based Image Steganography Using Run Length Encoding And Random Insertion Technique For Color Images. *Computer Science & Information Technology (CS & IT)*, 1(1):75-82.
- Elshazly, E., Abdelwahab, S., Abouzaid, R., and Sayed, M. E. (2018). A secure image steganography algorithm based on least significant bit and integer wavelet transform. *Journal of Systems Engineering and Electronics*, 29(3):639-649.
- Riza, B. S., Mashor, M. Y., & Haryanto E. V. (2019). The application of RSA and LSB in Securing Messages on Images. *ADI Journal on Recent Innovations*, 1(1):20-32.
- Denis, R. & Madhubala, P. (2020). Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment. *International Journal of Computer Networks and Applications (IJCNA)*, 7(6):208-230.
- Fahrul, I. L., Saib, S., & Poltak, S. (2021). Analysis of LSB Algorithm Modification with Bit Inverse and Insertion based on Length of Message. *n Proceedings of the International Conference on Culture Heritage, Education, Sustainable Tourism, and Innovation Technologies (CESIT 2020)*, 522-529.
- Kemal, T., & Özcan, C. (2021). Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach. *Computer Science and Information Systems*, 18(04):1311-1332.
- Osama, F. A., Aziza, I. H., Hesham, F. A. H., H. M. K., & Ashraf, A.M. K. (2020). Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. *IEEE Access*, 1(1):31805-31815.

- Pandikumar, T., and Tesfay, G. (2016). Information Security Using Image Based Steganography. *International Research Journal of Engineering and Technology*, 3(6):2839-2844.
- Deepa, S. (2015). A Prototype for Secure Information using Video Steganography. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(8):442-444.
- Provos, N., & Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *Hide and Seek: An Introduction to Steganography*, 1(3):32 - 44.
- IBM. (2021, November 2). *What is Data Security? Data Security definition and overview*. Retrieved from IBM: <https://www.ibm.com/topics/data-security>
- Arun, K, S., Juhi S., & Harsh, V. S., (2015). Steganography in Images Using LSB Technique. *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, 5(1):426-430.
- Mohammed, A. B., and Rossilawati, S. (2015). An Improved LSB Image Steganography Technique Using Bit-Inverse In 24 Bit Colour Image. *Journal of Theoretical and Applied Information Technology*, 80(2):342-348.
- Varsha, V., and Rajender, S. C. (2015). Data Hiding using Advanced LSB with RSA Algorithm. *International Journal of Computer Applications*, 122(4):41-45.
- Rachmawanto, B. S. (2020). Performance Analysis of LSB Color Image Steganography based on Embedding Pattern of the RGB Channels. *2020 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 1(1):73-78.
- Denis, R. & Madhubala, P. (2020). Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment. *International Journal of Computer Networks and Applications (IJCNA)*, 7(6):208-230.
- Khan, F. (2020). Prudently Secure Information Theoretic LSB Steganography for Digital Grayscale Images. *International Journal of Advanced Computer Science and Applications*, 11(8):594-614.