2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)

Improving The Hiding Capacity of Image Steganography with Stego-Analysis

1st Padmaja Grandhe
CSE Department
PSCMRCET
Vijayawada, India
padmajagrandhe@gmail.com

2nd A.Mallikarjuna Reddy
Department of CSE
Anurag University
Hyderabad, India

3rd Kavyasri Chillapalli
CSE Department
PSCMRCET
Vijayawada, India

4th Kavya Koppera
CSE Department
PSCMRCET
Vijayawada, India

5th Manasa Thambabathula
CSE Department
PSCMRCET
Vijayawada, India

6th L P Reddy Surasani
CSE Department
PSCMRCET
Vijayawada, India

2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS) | 979-8-3503-9846-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICICACS57338.2023.10100146

***Abstract*—Communicating online without fearing third-party interventions is becoming a challenge in the modern world. Especially the sectors like the military, and government organizations or private companies sharing sensitive information. They invest a lot of effort and cost into obtaining the advancement of safe communication techniques. Image processing encryption techniques using various algorithms promote security over communication channels and using different analysis methods make the tool stand out in providing security to the information. In today's world, there are various steganographic mechanisms that convert the secret message into stego medium and send it across various communication channels. Using algorithms like Blind Hide promotes the security of the message along with using multiple analysis methods that will further improve the tool in giving out information of encoded accuracy, size of stego of the secret message. The aim is to generate a tool that will give out a benchmark value of how precisely the message is stored in the cover file. Using Stego and bulk analysis the information about the presence of the stego medium in the message can be known to the user. All these analysis methods make the tool more enhanced and secure.**

Keywords—Cryptography, Digital image processing, Blind Hide Algorithm, Encryption, steganography, stego-image, Bulk Analysis, Benchmark Analysis, Stego Analysis, Decryption.

I. INTRODUCTION

Cryptography protects the data from the sight of third parties. It deals with the process of encoding the message in the form of ciphertext using symmetric and asymmetric cryptographic algorithms. The risk factor with this mechanism is that it allows the malicious users to “know” that there is a secret message that’s being transferred between users. In the case of steganography, concealing of message in another medium (usually referred to as stego medium) that promotes security in such a way that there can be no case of suspicion of a transfer of the message to an unauthorized party. Using various analysis mechanisms based on steganography can achieve secure communication.

Steganography is a method of protecting confidential messages from third parties. This is distinct from cryptography, which is a tool used to secure the information and for encrypting and decrypting data. Steganography is a method of concealment and deception. This is a method of closet information during the messages are secured using whatever medium, because no data is scrambled or a key’s used, it’s not a kind of cryptography. Instead, it is a quite knowledge concealment which can be accomplished in deceptive ways. Whereas cryptography may be a science that largely protects privacy, steganography may be a practice that protects confidentiality.

The goal of DIP is to manipulate images in order to modify or extract useful information from them. Digital image refers to discrete image elements called pixels. These pixels are represented by Digital Number (DN), which can be used to identify them. The use of a computer to process graphical images is known as digital image processing. It is critical to understand that a digital image is made up of a limited number of constituents, every element has its specifications. These include picture constituents, image elements, pels, and pixels.

The aim is to send a secret message over a communication channel without raising suspicion. This is where steganography comes into play. The various outcomes that come out of using this technique for sending secret message include avoidance of snooping of data. Since the data is hidden from plain eye sight, it can be assured that data is sent securely over different kinds of communication channels. The received output i.e., the stego-image resides in RGB speculation via preprocessing techniques. The various characteristics of steganography will result the RGB based image to give out less distorted image. But to achieve this size of the cover image should be larger than the size of the secret message to be passed, thus achieving less distortion. Another character of steganography is robustness. Using right algorithm should result in a robust stego-image, i.e., even if any circumstances occurs like scaling, cropping, the message should not modify and stay robust. Also, a stego-image should be tamper-resistant so that any attack from third parties will not destroy the original data. Steganography has various applications that include watermarking techniques that promote copy prevention control or broadcast monitoring. In the fields of data security, tamper resistance, source tracing and authentication methods come in hand.

II. RELATED WORK

[1] Taha et.al, Steganography is about communication in disguise. This paper explains how important it is to include steganography for a safer communication because no one can suspect the transmission of secret data. Alongside the usage of cryptography results in better encryption of the secret image. The main goal of steganography and cryptography is to achieve confidentiality and integrity. The aim is to prevent unauthorized users to access the data. These two techniques will result in better communication by promoting enhanced

979-8-3503-9846-5/23/$31.00 ©2023 IEEE

security. It provides security in which no one can access the secret information[17].

[2] AlKhodaidi et.al, There are some important multi-media is existed in security purpose. Counting-based secret sharing is fetching an imperative effective intermedia technique for increasing the security of delicate information. This paper focuses on how better the image can be redistributed using the LSB bits. The goal is that the final stego image should be less distorted and more qualified in quality. The LSB technique uses the least significant bits and targets them to store data in them. This is the most prominent technique as the distortion can be very less when compared to normal ways The information can be in any format, not only text, including audio, video, bitmap, etc. The 1-bit process selects a single zero when generating a key, with fewer zeros resulting in less shares, while the 2-bit process uses the target key to generate shares for the users. To secure the data steganography plays an important role and it uses some multimedia files to secure the message[13-15].

[3] Chandra et.al, One of the most important factors is data, and the quantity of data is used to organize the work. To ensure data security and prevent unauthorized information access. As a result, an image steganographic algorithm is developed that incorporates both cryptography and steganography. This algorithm takes input as text that is covered by the covered image and converts it to a stego image that is sent from sender to receiver. JPEG, BMP, GIF, MP3, txt, and other multimedia formats Because of their high degree of redundancy and popularity on the internet, these formats are appropriate as input messages. LSB coding, Phase coding, spread spectrum, and video steganography are examples of audio steganography. In the suggested method, firstly encryption of the plain text with a public key encryption algorithm, then select the cover image and generate the stego image [11],7[12]. To hide one image in another image file, steganography is offered, and watermarking is used to disguise the watermark image from the stego image. The RSA (Rivest, Shamir, and Adleman) algorithm is employed, Image steganography, and RMI (Remote Method Invocation) architecture to construct this methodology. Encryption of text data is done via the RSA algorithm.

[4] Purwantoro et.al, Great encoding algorithms like Blindhide and Filterfirst which promote excellent security to the secret message. This process consists quality and quantitative testing of an image on each Blindhide and Filterfirst algorithm. BlindHide is a well-versed technique that targets the starting pixels of an image. This method deciphers images by comparing the bits in each pixel with the bits in the secret message, and then going across and down the image bit by bit to find the matching image bit characters. It follows the main bit shift of the pixel colour to correspond with the hidden message. But there can be a few flaws such as not targeting any pixels but blindly storing information in the starting pixels[10,11]. It can be assured that the information is retrieved by the filter first from similar pixels and it cannot changed when hiding process is under processing. It can remove the unwanted data from the process such as the original image. The message is hided in any multimedia is very easy and safer way by using this algorithm[16].

[5,6] To perform steganalysis, first pick and extract a subset of features from the cover/stego media, and then inspect those features for any alterations. Targeted steganalysis and global steganalysis are the two primary categories of steganographic techniques, both of which are divided by specific domains of use. The first step in detecting steganography is to extract features from the input medium. These features are then evaluated and categorised. There are two categories of features: those that are deep and those that are handcrafted. In the first, well-known traits, such statistical ones, are retrieved by hand[7,8, 9]. Instead of being set by hand, deep features are extracted automatically via Neural Networks or deep autoencoders. Due to their prevalence as carrier files, digital media such as video, audio, and photographs must be subjected to steganalysis. Thus, the focus of this research is on steganographic techniques for digital media. The primary contributions of the survey are discussed in the next section.

TABLE. I. COMPARATIVE STUDY ON STEGANOGRAPHIC TECHNIQUES

S.No	Author Name	Algorithm	Advantages	Disadvantages
1.	Taha	Asymmetric encryption algorithms (AES). Secret encryption algorithm (SEA). Key-based security algorithms.	Robust and faster encryption.	Difficult to implement. High maintenance.
2.	Al Khodaidi	Least Significant Bit (LSB).	Easy to implement.	Vulnerable to steganalysis and not secure.
3.	Chandra	RSA algorithm.	Easy to implement and cracking is difficult due to its complexity.	Takes a long time to encrypt and process the message.
4.	Purwantoro	BlindHide algorithm, FilterFirst algorithm.	Blinde Hide is an easy implementation and is applicable for small stego objects. The FilterFirst algorithm adds the benefit of not needing a reference to the original object to decode.	BlindHide alone is a weak approach, as the stego image is going to have a large distortion on large data.

5.	Shehab	Stego Analysis.	Determines the existence of the stego medium in any medium (video, image, audio, text) and displays results.	The modern stage has increased the likelihood of criminals abusing this algorithm.

III. Proposed Method

This section will provide extensive detail on the method that was presented. These techniques, as stated previously, rely on LSB substitution with some bits' meanings being inverted. The image is split into two parts: one is used embed the secret message, and the other is used to manipulate the value of certain bits including the secret bits that were obtained through the LSB replacement technique. To identify which change was implemented to each pixel in the first part, use the other part. Better secret information concentration per square in the main image and improved stego image quality are two main benefits of the suggested strategy. Phases one and two are really the embedding and extracting phases..

Embedding process: There are two entry points into the embedding procedure used to conceal information. The first is used to encrypt the image data pertaining to the information, while the second is used to encrypt the image data pertaining to the cover. Fresnelet, a transform based on the Haar wavelet, is used to deconstruct data in order to protect its confidentiality. At first, the information image data fis propagated by the Fresnelet transform FT_{τ} with the first distance parameter key, $d_1 = 1\ m$, as (1),

$$FT_{\tau}(f, d_1) = \begin{pmatrix} ft_{\tau,d_1}^{(ll)} & ft_{\tau,d_1}^{(hl)} \\ ft_{\tau,d_1}^{(lh)} & ft_{\tau,d_1}^{(hh)} \end{pmatrix} \quad (1)$$

In the next stage, generate a scrambled data D from the decomposed data of of f by using the inverse Fresnelet transform IFT_{τ} with the second distance parameter key, d2 = 10−4 m, as (2).

$$D = IFT_{\tau}\left\{\begin{pmatrix} ft_{\tau,d_1}^{(ll)} & ft_{\tau,d_1}^{(hl)} \\ ft_{\tau,d_1}^{(lh)} & ft_{\tau,d_1}^{(hh)} \end{pmatrix}, d_2\right\} \quad (2)$$

Because of the way the Fresnelet transform works, the garbled information has complex values. Separate this complex data into the real part Dre and the imaginary part Dim for embedding those data into suitable detail subbands of the decomposed cover data as equation (5) and equation (6). To obtain the subband images into which the coded information data will be integrated, the WT is applied to a provided cover image CC. Imagine that the cover image's highest possible resolution is j. Four subbandpictures at the lower resolution level j−1 are created as follows by doing a one-level decomposition of CC as (3)

$$WT(C) = \begin{pmatrix} C_{j-1}^{(ll)} & C_{j-1}^{(hl)} \\ C_{j-1}^{(lh)} & C_{j-1}^{(hh)} \end{pmatrix} \quad (3)$$

Using a low-pass wavelet filter applied in parallel to the CC rows and columns, an approximated data $C_{j-1}^{(ll)}$is obtained. A horizontally oriented detail image data $C_{j-1}^{(lh)}$ is generated by applying the low-pass wavelet filter along the rows and the high-pass wavelet filter along the columns of CC. Similarly, a vertically oriented detail image $C_{j-1}^{(hl)}$ is obtained. By applying the high-pass wavelet filter along the rows and columns of CC, a detailed image data $C_{j-1}^{(hh)}$ is also obtained.

Notice that the approximated data $\mathrm{C}_{\mathrm{j-1}}^{(\mathrm{ll})}$is the low-pass subband image data containing high energy. Magnify it to the size of the original cover image by using bi-cubic interpolation and discard all high-passed details $\mathrm{C}_{\mathrm{j-1}}^{(\mathrm{hl})}, \mathrm{C}_{\mathrm{j-1}}^{(\mathrm{lh})}, \mathrm{C}_{\mathrm{j-1}}^{(\mathrm{hh})}$. The resized data R of $\mathrm{C}_{\mathrm{j-1}}^{(\mathrm{ll})}$is again decomposed into four subbands by using the WT as (4).

$$WT(R) = \begin{pmatrix} R_{j-1}^{(ll)} & R_{j-1}^{(hl)} \\ R_{j-1}^{(lh)} & R_{j-1}^{(hh)} \end{pmatrix} \quad (4)$$

Thesubband data $R_{j-1}^{(ll)}, R_{j-1}^{(hl)}, R_{j-1}^{(lh)}$ and $R_{j-1}^{(hh)}$are the low-passed image data, the horizontal detail image data, the vertical detail image data, and the diagonal detail image data, respectively. Note that the significant coefficients in the high-passed subband data are corresponding to edges, corners, and textures. So, embed the scrambled information image data into the subband data $R_{j-1}^{(hl)}$, $R_{j-1}^{(lh)}$. The real part Dreof the scrambled data is embedded into the subband data $R_{j-1}^{(hl)}$,$R_{j-1}^{(lh)}$, whereas the imaginary part Dimof the scrambled data is embedded into the subband data $R_{j-1}^{(lh)}$ as (5) and (6).

$$\tilde{R}_{j-1}^{(hl)} = R_{j-1}^{(hl)} + \alpha D_{re} \quad (5)$$

$$\tilde{R}_{j-1}^{(lh)} = R_{j-1}^{(lh)} + \alpha D_{im} \quad (6)$$

where the altered subband data R (j-1)((hl)) and R (j-1)((lh)) contain the false information data. A considered a wide range between 0 and 1 is generated by the equation (5-6) It is included as a strength variable with the goal of controlling the degree of encrypted data embedding. For embedding the bogus information data, the suggested method calculates mechanically based on Differential Evolutionary (DE), as indicated below. Through continuous natural selection refinement, this metaheuristic search method utilizes a population to generate a scaling factor.

The Technique of Embedding: We presume that perhaps the cover image's pixels comprise up to 256 shades of grey. Based on the size of the imbedded data, Table 1 displays how the watermark image is split into two parts.

In the cover design, the quantity of bits of something like the secret message will firstly be fixed to all pixels and will be implanted to each cell Pi with a grey value of yi. Block the kdimensional secret message into pieces. Replace each block in the first segment into the k LSB of yi, yielding y′ .

Invert all (k 1, k) th bits of the k LSB of y. Each of the y"i acquired in step 3 should indeed be treated to the best LSBs algorithm. We currently have two pixel values. – In their place, enter the number that comes the closest to the original value, yi. Then, to indicate which change was picked, return 0 or 1. - We start at the end of the second section. The change that was made to one pixel in the first section is expressed by each bit of the LSB of any and every pixel in this section. Along with the indicator in the pixel's o LSB. Then, employ the best LSBs approach for each pixel. – Continuation of the previous stages is essential to embed the entire secret message.

A. *Initialisation*

In DE, the search for a global optimum solution takes place in a D-dimensional space of parameters, and the first step in this process is called "initialization." During the initialization phase, the limits of the search space are used to generate the first set of solutions.

B. *Mutation*

Evolutionary computation's mutation process involves randomly adjusting the scale parameter.

C. *Crossover*

Here, the mutant and target vectors jointly cross their respective scaling factor ranges to generate a test vector via a probabilistic process (offspring).

D. *Selection*

DE's population size is maintained in each generation thanks to the selection process, which determines whether or not a target (parent) or trial (offspring) key will persist into the following search iteration (X_i^{t+1}). Following the formation of the new population in the subsequent generation, mutation, crossover, and selection are repeatedly used until the termination requirements are met..

Instead of using the resized data $R_{j-1}^{(ll)}$ during the reconstruction process, use the approximate data $C_{j-1}^{(ll)}$ to the original cover artwork to improve stealth and ensure that any fake data is successfully extracted as (7).

$$E = IWT\begin{pmatrix} C_{j-1}^{(ll)} & \tilde{R}_{j-1}^{(hl)} \\ \tilde{R}_{j-1}^{(lh)} & R_{j-1}^{(hh)} \end{pmatrix} \tag{7}$$

The following reconstruction method with the inverse wavelet transform (IWT) gives an information embedded picture EE after embedding the real and imaginary sections of DD in the selected bands of CC.

E. *Extraction process*

As the opposite of embedding, extraction involves taking out the original. Image E is decomposed into four subbands using the wavelet transform (WT). $E_{j-1}^{(ll)}$, $E_{j-1}^{(hl)}$, $E_{j-1}^{(lh)}$ and $E_{j-1}^{(hh)}$. The high frequency subband data $E_{j-1}^{(hl)}$&$E_{j-1}^{(lh)}$ are information are preserved in the same position. By using the bi-cubic interpolation, resize the low-pass subband data $E_{j-1}^{(ll)}$ with the same size as that of the input embedded image. In order to extract the embedded information data, the WT is applied again to the resized data E_r and then obtain the following four subband data $E_{j-1}^{r(ll)}$, $E_{j-1}^{r(hl)}$,$E_{j-1}^{r(lh)}$ and $E_{j-1}^{r(hh)}$.

The scrambled data (with real and imaginary parts) can be extracted by subtracting the high frequency subband data $E_{j-1}^{r(lh)}$ and $E_{j-1}^{r(lh)}$ from the data $E_{j-1}^{r(lh)}$ and $E_{j-1}^{r(hl)}$ of the information embedded image, respectively. Afterwards the difference net data are divided by α so that the scrambled information data is obtained. A complex data set is the result of him piecing together the genuine and fictional pieces of the original scrambled data. Finally, the secret information image is extracted from the complicated scrambled data by use of the inverse Fresnelet transforms, employing the same parameter keys as the Fresnelet transform.

F. *Extraction Algorithm*

To establish which changes have been made in order to restore the original secret data, the original image I must be known. The following steps must be followed at the receiving end:

Beginning at the end of stego image I' and compare each pixel's LSB to its corresponding pixel in image I. The (k-1)th bit is inverted if two bits are identical to each other. If not, the bits are reversed (k-1, k). We can get the secret data by flipping the value of the first part's bits after determining out which adjustments have actually occurred. The LSB of the stego-k-bit bitmap includes the k-bit secret message. The retrieval algorithm then completes, obtaining all of the secret data.

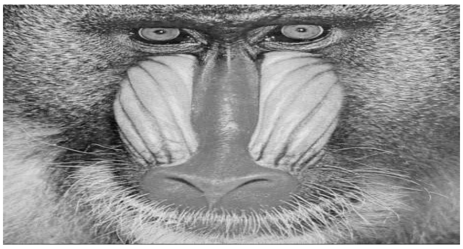
IV. Results Analysis And Discussion

Six experiments are conducted to evaluate our proposed scheme. In the trials, cover images with the usual grayscale representation of Lena, Baboon, "Pepper," "Barbara," "Elaine," and "Cameraman" with widths 512 x 512 and 128 x 128 of each are employed. The cover designs include embedded pseudo-random binary numbers that symbolize the secret bit streams.

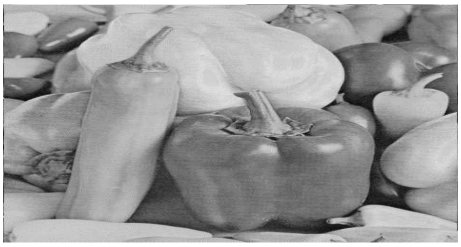
Fig. 1 illustrates six 512 by 512 cover designs. Lena, Baboon, Peppers, Barbra, Lorraine, and Photographer are really just some few choices.

The data quantity as well as the visual quality of the stego image are two metrics used it to assess project.

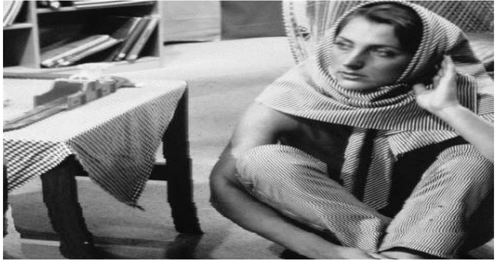
a. Lena



b. Baboon



c. Peppers



d. Barbara

e. Elaine

f. Photographer

Fig. 1 Six cover images with size 512 x 512

Standard test photos of Lena, Baboon, and Pepper (each 512 pixels on the longest side) were used as covers in the following series of trials. Both the 8-bit and the 16-bit cover formats were tested. In addition, the hidden message was a 512 × 512. pixel image with 8 bits of colour depth. Fig. 1 displays these pictures. Matlab's image processing tool box was used to create implementations of the hiding and extraction methods. In addition, all experiments were performed using the principles of the Haar transform.

The results of the proposed approach are presented in Table II along with the embedding capacity (in bits) and Speckle noise value. Images with a size of 512 512 been selected. In this table, "k" and "o" stand for the number of LSB in the cover images pixels in the first and secondary portions, respectively, and "C" stands for the capacity of hidden data. The results for "C1" are "349524," "C2," "589824," "699048," "786432," "838860," "873810," "983040," "C9," and "1092265."

TABLE. II. EXPERIEMENT RESULTS

CIs	**P** **K=2** **o=2** $C = C_1$	**P** **K=3** **o=2** $C = C_2$	**P** **K=3** **o=3** $C = C_3$	**P** **K=4** **o=2** $C = C_4$	**P** **K=4** **o=3** $C = C_5$	**P** **K=4** **o=4** $C = C_6$	**P** **K=5** **o=2** $C = C_7$	**P** **K=5** **o=3** $C = C_8$	**P** **K=5** **o=4** $C = C_9$	**P** **K=5** **o=5** $C = C_{10}$
Lena	49.85	46.57	44.43	41.97	40.78	38.84	36.42	35.72	34.84	33.10
Baboon	49.91	46.55	44.40	41.97	40.78	38.85	36.42	35.72	34.83	33.11
peppers	49.92	46.54	44.41	41.94	40.77	38.83	36.42	35.70	34.83	33.11
Barbara	49.90	46.54	44.42	41.93	40.77	38.84	36.40	35.69	34.82	33.07
Elaine	49.89	46.54	44.42	41.96	40.78	38.84	36.43	35.71	34.88	33.11
Photographer	49.90	46.57	44.42	41.97	40.79	38.87	36.45	35.74	34.88	33.14

Image quality is degraded when using the steganography method of concealing information inside the image's pixels. A modified image must remain undetectable to invaders. Mean square error (MSE), peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and other standardised evaluation methods are used to verify the strength of the image quality.

A. *Mean square error (MSE)*

The mean squared error (MSE) is used to quantify the degree to which the stego image deviates from the source image. It's useful for contrasting the pixel values of the original with the stego. Higher image quality is attained with smaller MSE values. Therefore, the MSE value should be near '0'. MSE can be calculated as (8).

$$MSE = \frac{\sum_{i=1}^{n}(p_i - p_i')^2}{n} \tag{8}$$

where $p_i \& p_i'$ denotes the pixel values of the original and stego image, n represents the image size.

B. *Peak signal to noise ratio (PSNR)*

PSNR is a metric for gauging visual quality that can be used to compare the stego image to its source. It makes an approximation of how many pixels in a stego image are different from the original. The PSNR value should be greater than 39dB [9] for higher image quality as (9).

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{9}$$

C. *Structural similarity index (SSIM)*

To determine how close an original and stego picture are to one another, SSIM is used as a visual quality measuring technique. Image quality is considered to be high when the SSIM value is near to '1' (means 100%) [10]. In mathematics, SSIM looks like (10)

$$SSIM(i,j) = \frac{(2\mu_i\mu_j + C_1)(2\sigma_{ij} + C_2)}{(\mu_i^2 + \mu_j^2 + C_1)(\sigma_i^2 + \sigma_j^2 + C_2)} \tag{10}$$

where μ_i and $\mu_j$are the mean intensity, σi and σj are the standard deviations, and σ_{ij} is the cross-covariance of images i and j respectively.

TABLE. III. PARAMETER COMPARISON OF EXISTING IMAGE STEGANOGRAPHY TECHNIQUES

Algorithm	PSNR (dB)	MSE	SSIM
RSA	36.82	5.2123	0.8141
Blind Hide algorithm (BHA)	38.63	3.1019	0.8512
Filter First algorithm (FFA)	40.71	1.2140	0.8717
Differential Fresnelet Wavelet transform (DFWT)	43.54	0.8541	0.9263

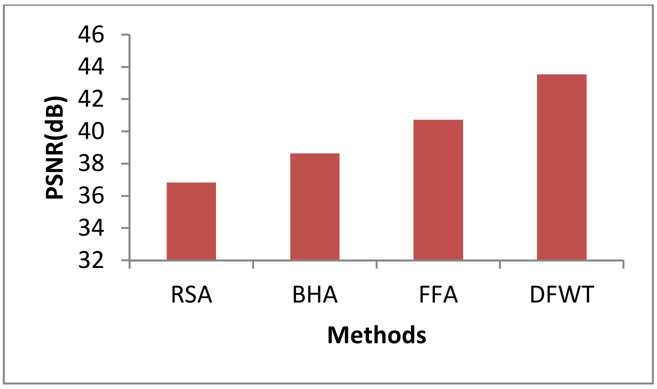


Fig. 2 PSNR compariosn of steganography techniques

Fig. 2 and table III shows the PSNR comparison of various stegonography methods. From the resutls it shows that the proposed system has higher results if 43.54 dB, whereas other methods such as RSA, BHA, FFA has lesser value of 36.82 dB, 38.63 dB, and 40.71 dB.

V. CONCLUSION AND FUTURE WORK

In this research, we present a blind data hiding strategy that greatly improves the invisibility of the embedded information data while maintaining its high storage capacity. Differential Fresnel Wavelet transform (DFWT) is implemented for processing data in order to deconstruct and recreate the cover photograph. When it comes to DFWT, the lifting framework is used because of its low computational complexity and negligible storage overhead. DFWT is used to encode secret information in the form of complicated fake data in the cover picture data using a variety of keys while maintaining the data's overall energy. Researchers can improve steganography performance by creating ensemble algorithms or deep learning algorithms for data concealing.

REFERENCES

[1] Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., &Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A Short Survey. IOP Conference Series: Materials Science and Engineering, 518, 052003. doi:10.1088/1757-899x/518/5/052003

[2] AlKhodari,T., Gutub, A. Refining image steganography distribution for higher security multimedia counting-based secret-sharing. Multimed Tools Appl80, 1143–1173 (2021). https://doi.org/10.1007/s11042-020-09720-w

[3] Nalla, Pattabhi Ramaiah, and Krishna Mohan Chalavadi. "Iris classification based on sparse representations using on-line dictionary learning for large-scale de-duplication applications." Springerplus 4, no. 1 (2015): 1-10.

[4] Purwantoro, &Garno, Garno&Sunita, Ari. (2020). A Comparative Study of Blindhide and Filterfirst Algorithm in Digital Images for Steganography Techniques. 10.4108/eai.12-10-2019.2296320.

[5] Shehab, D.A.; Alhaddad, M.J. Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research. Symmetry2022, 14, 117. https://doi.org/10.3390/sym14010117.

[6] A.Mallikarjuna, B. KarunaSree, " Security towards Flooding Attacks in Inter Domain Routing Object using Ad hoc Network" International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-3, February 2019.

[7] A. Mallikarjuna Reddy, V. Venkata Krishna, L. Sumalatha," Face recognition based on stable uniform patterns" International Journal of Engineering & Technology, Vol.7 ,No.(2),pp.626-634, 2018,doi:10.14419/ijet.v7i2.9922

[8] Kumar, G. H., & Ramesh, G. P. (2017, February). Intelligent gateway for real time train tracking and railway crossing including emergency path using D2D communication. In 2017 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-4). IEEE.

[9] Sukumar, A., Subramaniyaswamy, V., Vijayakumar, V. and Ravi, L., 2020. A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage. Multimedia Tools and Applications, 79(15), pp.10825-10849.

[10] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S. and Baik, S.W., 2018. Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Generation Computer Systems, 86, pp.951-960.

[11] M. H. Marghny, N. M. AL-Aidroos, and M. A. Bamatraf "A Combined Image Steganography Technique Based on Edge Concept & Dynamic LSB." International Journal of Engineering Research and Technology, Vol.1, No. 8, ESRSA Publications, 2012.

[12] H. W. Tseng and H. S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," Hindawi Publishing Corporation, Journal of Applied Mathematics, vol. 2013, no. 13, pp. 1-8, 2013.

[13] Kang, H.; Wu, H.; Zhang, X. Generative text steganography based on LSTM network and attention mechanism with keywords. Electron. Imaging 2020, 2020, 291.

[14] S. Begum, R. Banu, A. Ahamed and B. D. Parameshachari, "A comparative study on improving the performance of solar power plants through IOT and predictive data analytics," 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), Mysuru, India, 2016, pp. 89-91, doi: 10.1109/ICEECCOT.2016.7955191.

[15] Hamzah, A.A.; Khattab, S.; Bayomi, H. A linguistic steganography framework using Arabic calligraphy. J. King Saud Univ.-Comput. Inf. Sci. 2021, 33, 865–877.

[16] Li, Y.; Zhang, J.; Yang, Z.; Zhang, R. Topic-aware neural linguistic steganography based on knowledge graphs. ACM/IMS Trans. Data Sci. 2021, 2, 1–13.

[17] Zhou, X.; Peng, W.; Yang, B.; Wen, J.; Xue, Y.; Zhong, P. Linguistic steganography based on adaptive probability distribution. IEEE Trans. Dependable Secur. Comput. 2021.