International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 11 | November - 2022 Impact Factor: 7.185 ISSN: 2582-3930

OPTIMIZED DATA HIDING IN IMAGE STEGANOGRAPHY USING IMPROVED JAYA ALGORITHM

Parwinder Singh[1], Kulwinder Singh[2]
[1, 2] Bhai Maha Singh College of Engineering, Sri Muktsar Sahib

***Abstract*:** Image steganography gains popularity to secure secret data by hiding in the cover image. However, the data hiding process generates variability in the cover image. In order to reduce variability, various approaches have been proposed. Some of the authors are deployed swarm intelligence algorithms to search the optimal starting pixel in the cover image/best pixels in the cover image. On the other side, some authors match the secret data bits with the cover image bits, and the optimal index is determined. After that, hide the optimal index in the cover image using the LSB algorithm that generates the variability in it. In the proposed method, both approaches are hybridized. Initially, the cover image is read and it is split into two regions known as smooth and edge. The secret data bits match with the smooth region pixels and the optimal index is determined. After that, optimal indexes are hidden in the edge region using an improved JAYA algorithm to reduce the variability in the cover image. Besides that, pre-processing of the cover image is done based on the human visual characteristics to select the most appropriate planes for hiding the optimal indexes. The subjective and objective analysis is done for the proposed method to validate its performance. In the last, the proposed method is compared with the existing method based on the PSNR parameter.

Keywords: Image Steganography, JAYA Algorithm, Modified Swap Operator, Optimized Data Hiding, Security.

1. INTRODUCTION

Users of the Internet nowadays are able to not only interact with one another, but also to exchange private and protected content with one another. Data security via the Internet, therefore, has become a big concern. The art and science of steganography depend in the ability to conceal sensitive information from those who should not have it. However, it's worth noting that the original picture is called "cover" when secret data is embedded into it, while the image that results after this process is called "stego." Steganography relies on the fact that only the intended receiver can decipher the hidden information [1]. There are several ways steganography may be used in the area data. While steganography has its origins in ancient Greece, it is now being studied for security purposes. Under steganography, message is hidden in a cover image like text, picture, audio, and video [2]. An encoded message may be hidden in an accompanying cover file before it is sent. As a result, it is only known or understood by the sender and the receiver, and not by any third-party observer. It is a hidden message (plain text) that is included inside a cover file by the sender. To decipher the coded code, a "stego-key" is used on the recipient's end.

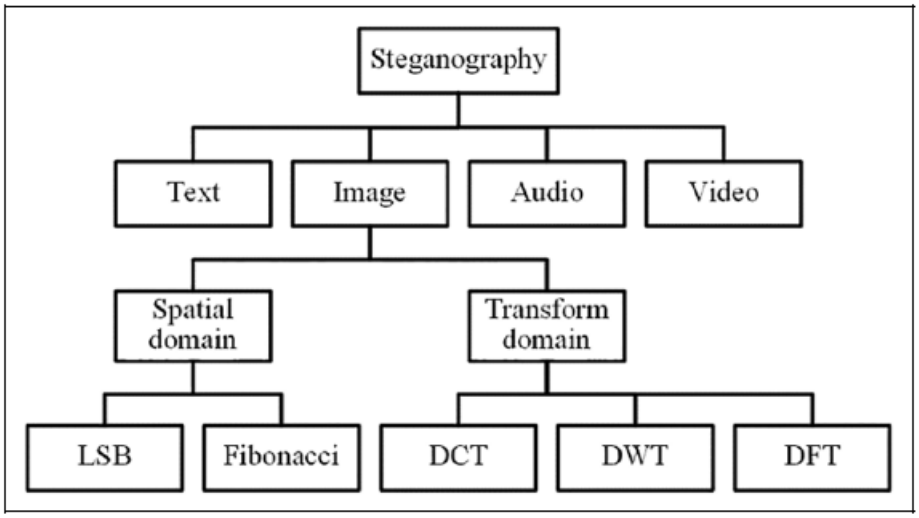

Figure 1: Various Types of Steganography Techniques [1]

These approaches have been extensively explored in the recent decade. A variety of steganographic methods are shown in Figure 1. Image steganography techniques may be divided into spatial and frequency domain based approaches [3]. The image's grey values may be altered directly via spatial domain steganography techniques. The frequency domain–based approaches, on the other hand, accomplish image alteration by translating the image into several transformations. The DWT, DFT, and Discrete Cosine Transform are all types of discrete wavelet transformation, respectively. There are different requirements for both spatial and frequency-based techniques. When it comes to hiding significant amounts of secret information and good quality stego

pictures, spatial steganography techniques may not be suitable for steganalysis. In contrast, frequency-based watermarking technologies are often used because they are resistant to image distortion.
In this paper, we have worked in the spatial domain of the image steganography. LSB is the most preferred method. However, this method provides variability if number of bits per pixel is increased from 1-bit to 2-4bits. In order to reduce variability, Pratik D. Shah and R.S. Bichkar [4], designed an matching method. In their method, one quarter part of the image is used for matching purposes whereas remaining part of the image is used to hide the optimal index. Using a genetic algorithm, the optimal index is hidden in the cover picture. Their strategy, on the other hand, results in a less potential for embedding.Further, Kamil et al. [5], designed a complemented or non-complemented method. In their method, complemented or non complementform of secret data is matched with cover image LSB bits. According to matching, optimal index is determined and hide in the cover image using k-bit LSB method. Their method provides better embedding capacity over the previous method [4] but LSB method optimal index hiding provide variability. Next, Sahil et al. [6], split the cover image into smooth and edge region. The smooth region is used to matching the secret data with cover image LSB bits whereas edge region is used to hide the optimal index determined from matching algorithm. However, their method embedding capacity depends on the number of edges in the cover image. In addition, LSB-based index concealment introduces unpredictability into the system. In the proposed methodology, these issues are taken into account.
The main contribution of this paper is to reduce the variability in the cover image. To achieve this goal, improved JAYA algorithm is taken under consideration. There are two stages to the approach that has been presented. Data bits and cover image pixels are matched during first phase and optimum matched indices are found. The revised JAYA method is used in the second stage to hide the optimally matched index from view in the cover picture. An updated version of the JAYA algorithm looks for the best beginning pixel in the picture.Besides that, the cover image is split into smooth and edge region. The smooth region pixels are used for matching purposes whereas edge region pixels are used for hide the optimal matching indexes. The standard dataset photos are used in the performance evaluation of the proposed methodology.The results presents that the proposed method is superior over method proposed by Sahil et al. [6] in terms of Peak Signal to Noise Ratio (PSNR).

The remaining paper is as follows. Section 2 defines the related work in which various approaches of data hiding are studied. Section 3 defines the preliminaries are required for the proposed method such as the HVS characteristics-based plane selection, JAYA algorithm, and LSB algorithm. Section 4 shows the proposed method. Section 5 illustrates the simulation evaluation of the proposed method.

2. RELATED WORK

This section shows the related work to study the existing data hiding approaches are proposed in the image steganography.

Pratik D. Shah and R.S. Bichkar [4], suggested that a image steganography method that is both secure and lossless. For each pixel, an appropriate position is identified to conceal two bits of hidden information, leading in a coefficient matching to the position of the secret information match. This LSB replacement steganography conceals the coefficients in the image's remaining part. Genetic algorithm was utilised to identify the optimal spot to conceal these coefficient in the image, making this suggested solution very safe and almost difficult to retrieve secret data from it. The suggested approach is compared to LSB replacement strategy of steganography, in which the same amount of secret information is implanted. When compared to LSB steganography, the suggested method seems to be a vast improvement. As a result, histogram attack is eliminated, and MSE and PSNR values are improved. In comparison to the LSB methodology, the PSNR value of the stego-image derived from the suggested method is 53.11dB at 2-bits pixels data embedding rate.

Kamil et al. [5], studied that in order to hide data accurately and improve the visual quality of steganography techniques, it was observed that the cover media must be perfectly matching. Cloud data security has recently seen the development of numerous improved steganography techniques, such as genetic algorithm (GA), least significant bit (LSB) match, and particle swarm optimization (PSO). Even though these algorithms are able to find the best possible match for the hidden data in the cover media, they take a lot of time to do so. Steganography techniques that can achieve practically zero variability and extremely low computing time were suggested in this study. To hide hidden data bits in complemented or non-complementary forms, video steganography was used to its full potential. For the complemented and non-complemented forms, this frame concealed indexes as well. This made it possible for the recipient to receive the secret communications quickly and effectively. There were a number of metrics used to evaluate the suggested algorithm's performance, including embedding capacity, peak signal to noise ratio (PSNR), average difference, normalised cross-correlation, and normalised absolute error. According to the findings, the suggested steganography system outperforms the already available state-of-the-art approaches. Using the technique created, cloud computing video data security is considerably improved.

Sahil et al. [6], studied that data hiding has been adjusted in light of HVS features in this research. Red, green, and blue (RGB) planes make up the colour picture. Human eyes are more sensitive to the green plane than the blue one. As a result, the green plane is utilized as a reference surface for information hidden in the blue and red planes in the newly suggested approach. The secret data bits in the optimal data concealing approach match the cover pixel values. Data hiding is done in cover pixels' LSB bits if the bits match, if not, the appropriate optimum index is determined. Afterwards, a 2-bit LSB method is used to conceal the

optimum indexes in the cover picture. Before hiding data, the proposed approach examines picture smooth and edge region features. The smooth zone has a high correlation between adjacent pixels, whereas the edges have a low correlation. To avoid detection, the ideal indexes have been hidden on the borders and all secret data has been matched to the cover pixel bits in the smooth area. An picture database of standard datasets used for the experiment. As contrasted to the currently used methods, the suggested strategy produces superior visual quality.

Pratik D. Shah and R.S. Bichkar [7], presented that steganography is a technique for encrypting messages. Steganography has a distinct advantage over other methods of covert communication since it is able to hide the fact that it is being used. Images are encoded with information that is difficult to decipher, but that has no effect on the cover picture. Image steganography is the subject of a great deal of study, but only a few studies have looked at the prospect of using a cover image for steganography that is more compatible with the hidden data than the default option. One may use a genetic algorithm to find the best cover picture from the library of photographs in this paper. The cover picture chosen is the best match for the provided secret data. They also look at the idea of reordering the secret data in order to make the stego picture more imperceptible.

Astuti et al. [8], studied that steganography relies heavily on its ability to remain undetectable. Steganography in photographs, in particular, necessitates that the human visual system not be able to detect any hidden signals. Because humans are more sensitive to colour pictures than to grayscale photos, the approach currently being evaluated on grayscale images should be retested on colour images. In grayscale pictures, the bit flipping approach has been demonstrated to boost imperceptibility by roughly 9dB. Bit flipping is tried on RGB colour pictures with a message capacity of 1 bit per pixel in this experiment. Because of the higher number of layers in a colour picture, the imperceptibility test yielded more diverse findings. Color pictures, on the other hand, may benefit from a maximum PSNR boost of more than 13dB using the bit-flipping approach. The message picture may also be properly extracted during the extraction step, specifically with the variable NC = 1.

3 PRELIMINARIES

This section explains the HVS characteristics-based cover image plane selection and an overview of the JAYA and LSB algorithms.

3.1 HVS Characteristics-based Cover Image Plane Selection

The Gamma radiation have a wavelength of 0.001 nm, while the Radio waves have a wavelength of 100 ft. The electromagnetic spectrum encompasses the whole range. In this lengthy spectrum, the visible spectrum is quite narrow and ranges from 380 and 780 nm [9]. There are just a few frequencies in the electromagnetic spectrum that can be seen by the average human eye. Each shade has a distinct visual spectrum that may be seen and recognized from one another. Red is the first colour that the human eye sees, and Violet is the last colour that it sees. This limited spectrum shows just the pure colours, whereas other colours appear as a blend of pure colours from other sources. In the end, the light that enters a human eye's pupil travels to the back of the eye and hits the retina, a membrane that senses light. Rods and cones are light-sensing cells in the retina of the eye, which explains why the retina is so sensitive. Intensity of light affects the rods, whilst various colours have a varied effect on the cones of the eye. The three sorts of cones are based on their ability to differentiate between different colours. Depending on the colour wavelength spectrum, each one has a different level of sensitivity to the other. There are three types of color-sensing cones: blue, red, and green. Figure 2 depicts the human eye's internal anatomy, including the rods and cones light sensors. As illustrated in Fig. 2, each of the three kinds of cones is sensitive to a particular range of wavelengths associated with its colors.

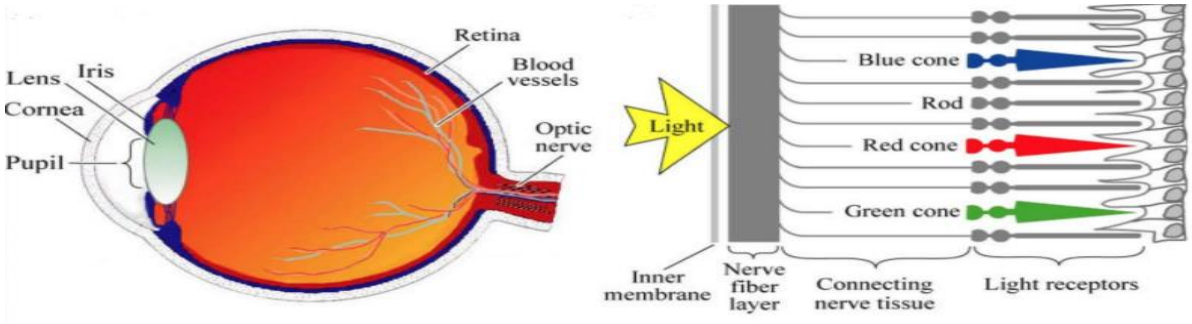

Figure 2: Structure of the Human Eye with rods and cones light receptors

Red cones, for example, are triggered by a mixture of red, orange, and yellow colours. Only a small percentage of the Red cones are triggered by the Green light. While blue and yellow wavelengths are stimulated by a green colour, the green cones are less reactive to them. Receptor pathways for each colour contribute to a single human subject's overall foveal sensitivities. The foveal sensitivity to colour channels is 0.053, Green is 0.575, and Red is 0.542 if a maximum value of 1.0 is supplied. The word

luminance (brightness) in the image analysis concept represents this colour sensitivity from a medical perspective. Red, Green, and Blue wavelengths are used to create the luminance L value for each each pixel, as indicated in the following equation (1).

$$L = (0.2126 \times R) + (0.7152 \times G) + (0.0722 \times B) \quad (1)$$

Color images may be converted into grayscale using (1), which takes into account the brightness of each individual colour channel. Three kinds of cones are shown in Figure 3 based on their sensitivity to light and the individual eye's sensitivity to each form of cone. The brightness of each pixel in a colour picture may be calculated using these numbers. For this reason, we have developed a new state of the art method for hiding a hidden message in a cover photo.

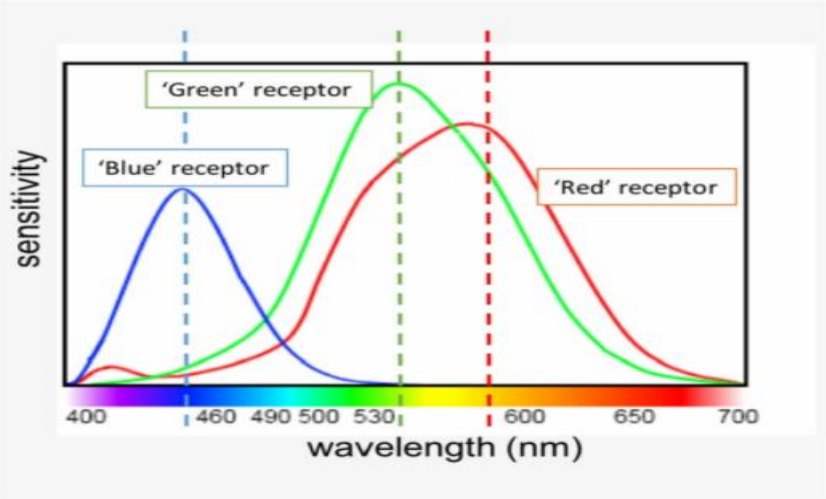

Figure 3: Spectral sensitivity of the RGB color cones [9]

The cover image's Blue channel may be used to initially hide the secret message if the viewer's eye is less sensitive to blue color. The Red colour is the second less sensitive channel, hence the Red channel is used to disguise the hidden message. Last but not least, we choose the Green channel since it's the most vulnerable to human eyes. Therefore, in the proposed method, green channel is used as a reference plane whereas blue and red planes are used for data hiding.

3.2 Improved JAYA Algorithm

In 2016, Rao presented the Jaya algorithm, a population-based meta-heuristic algorithm [10]. The other meta-heuristic algorithms have parameters to specify, while Jaya does not. It was designed to solve issues involving continuous optimization.Figure 4 shows the flowchart of the JAYA algorithm. The steps of JAYA algorithm is explained below.

Initialization. The first step of the algorithm is to randomly generate the initial population as x_{jk}^{t+1}, $j = 1, \ldots, m$, m represents the number of problem variables, $k = 1, 2, \ldots, SS$, and SS represents the size of population.

Population evaluating. At some iteration t, the population's solutions are evaluated. In this, the best and worst solutions are found represented as (x_{best}^{t}) and (x_{worst}^{t}).

Solutions updating. In the next step, every solution of the population is updated. This updation is based on the best and worst solutions found from previous step. It is described using Eqn. 2 as follows:

$$x_{jk}^{t+1} = x_{jk}^{t} + r_{1j}^{t}\left[\left(x_{j,best}^{t}\right) - \left|x_{jk}^{t}\right| - r_{2j}^{t}\left[\left(x_{j,worst}^{t}\right) - \left|\left(x_{jk}^{t}\right)\right|\right]\right] \quad (2)$$

where r_{1j}^{t} and r_{2j}^{t} represents the random numbers that are in range [0, 1]. In case when the new solution is more optimized then the previous one, the new solution then becomes the current best solution.

Termination criteria Until the termination requirements have been met, the preceding procedures are repeated.

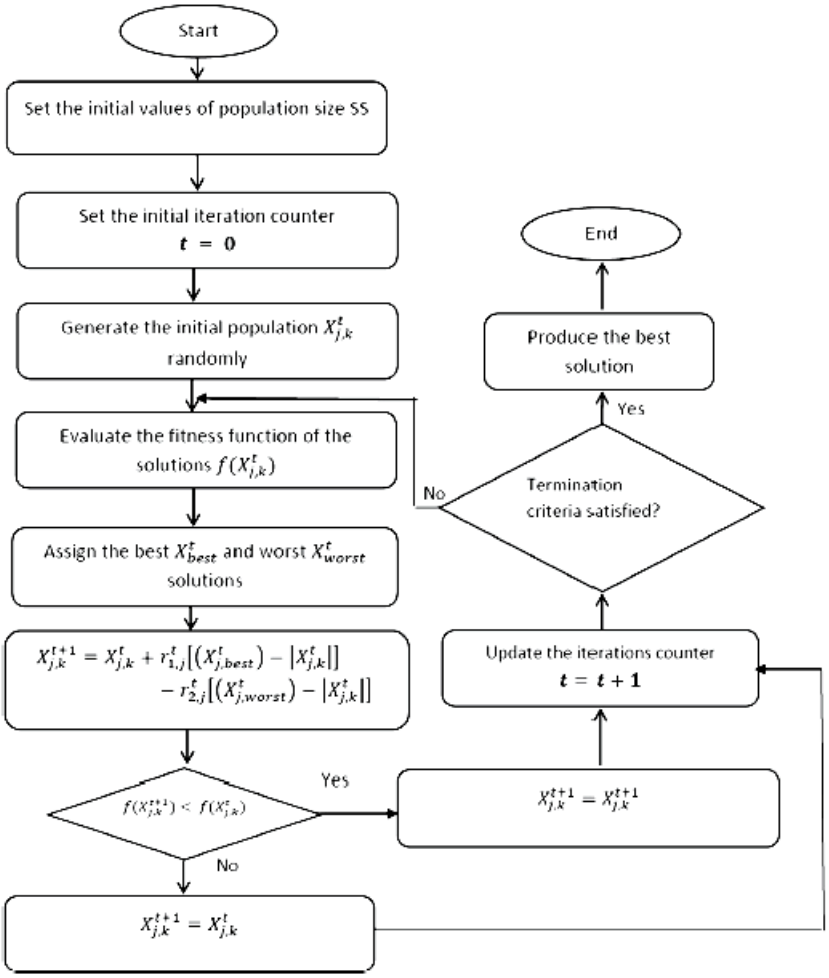

Figure 4: Flowhart of the JAYA Algorithm [10]

In the improved JAYA algorithm, equation 2 is updated using modifed swap operator (Eqn. 3).Using MSO, teams may exchange experts (2nd and 3rd indices) who have the same expertise (the first index) as each other. This ensures that the answer is legitimate in terms of the expertise of each expert.

$$x_{jk}^{t+1} = x_{jk}^t \oplus r_{1j}^t \otimes [x_{j,cross}^t - x_{jk}^t] - r_{2j}^t \otimes [x_{j,worst}^t - x_{jk}^t] \quad (3)$$

where "⊕" is a combining operator of two swap operators. The mark "⊗" means the probability of r_{1j}^tthat all swap operators are selected in the swap sequences $x_{j,cross}^t - x_{jk}^t$and the probability of r_{2j}^tthat all swap operators are selected in the swap sequences $x_{j,worst}^t - x_{jk}^t$.

3.3 LSB Algorithm

LSB is the most preferred algorithm in the steganography [11]. In this algorithm, least significant bit of the cover image pixel is replaced with secret data bit, as shown in Figure 5. In the proposed method, k-bit LSB algorithm is used to hide the optimal indexes in the cover image.

10100011	11001010	00110011	10100011

(a) Cover Image Pixels

0	1	0	1

(b) Secret Data Bits

10100010	11001011	00110010	10100011

(c) Stego Image Pixels

Figure 5: LSB Algorithm

4. PROPOSED METHOD

The main aim of the proposed method is to design an approach that reduces the variability in the cover image, that generated due to the data hiding process. The block diagram of the proposed method is shown in Figure 5.

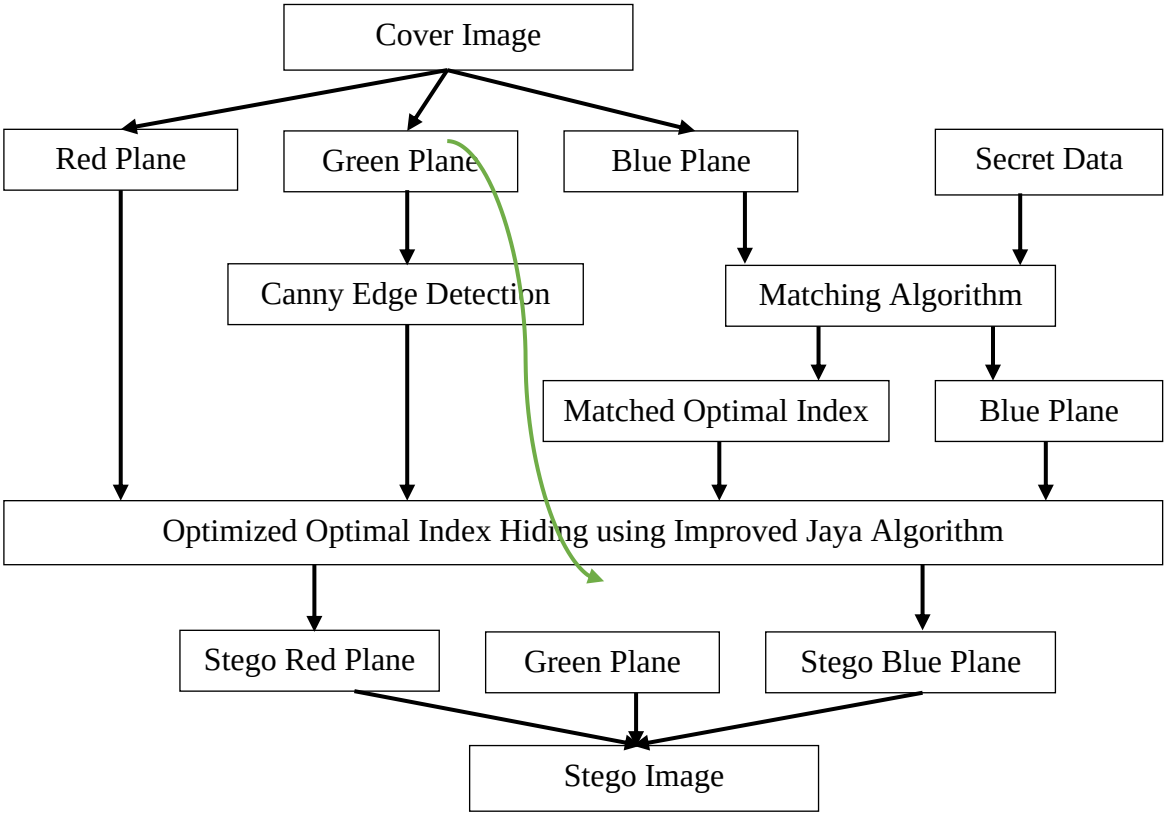

Figure 6: Flowchart of the Proposed Method

Initially, the cover image is read and extract its RGB planes. After that, based on the HVS characteristics, red and blue planes are chosen for the data hiding process and green plane is used as a reference plane. We have applied canny edge detection algorithm on green plane and determine smooth and edge region. Thereafter, secret data is read and matched with smooth region pixels of the blue plane and optimal indexes are determined. After that, red and blue planes edge pixels are read along with optimal indexes are given to the improved JAYA algorithm. In order to conceal the ideal index, JAYA's updated algorithm looks for the optimal beginning point in the edges. Finally, a subjective and objective analysis is used to assess the method's performance.

5. SIMULATION EVALUATION

This section shows the simulation evaluation of the proposed method. The algorithm is simulated in MATLAB. The simulation setup configuration for the proposed method is shown in Table 1.

Table 1: Simulation Setup Configuration

Parameters	Value
Total Population	30
Iterations	100
r1 and r2 Constant	[0-1]
Crossover	Single Point
Cover Image	SIPI Image Database [12]
Secret Data	Randomly Generated for Validation Purposes

Further, subjective and objective analysis is done for the proposed method to evaluate its performance.

5.1 Subjective Analysis

In the subjective analysis, cover and stego images are compared based on visual quality between them [13]. Due to the data hiding process, variability is generated in the stego image that negatively impacted the visual quality. Therefore, subjective analysis is shown for the proposed method in Table 2. The results show that the cover image and stego image looks similar.

Table 2: Subjective Analysis for the Proposed Method

Cover Image	Stego Image
	
	
	
	
	

5.2 Objective Analysis

In the objective analysis, various parameters are determined for the proposed method. A detailed description of the parameters is given in Table 3.

Table 3: Detailed Description of the Parameters [14-15]

Parameter	Equation
Mean Square Error (MSE)	$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij} - S_{ij})^2}{M \times N}$
Peak Signal to Noise Ratio (PSNR)	$PSNR = 10\log_{10}\frac{Peak^2}{MSE}$
Embedding Capacity (EC)	The total number of bits can be embed in the cover image. In the proposed method, 3-bits per pixel is hide.

Note: CN denotes the cover and stego image. MN denotes the size of the cover image. $Peak$ denotes the maximum pixel, we can represent in the image.

Table 4 shows the objective analysis of the proposed method. The result shows that pepper image achieves the highest PSNR whereas baboon image achieves the lowest PSNR. Besides that, baboon image achieves highest embedding capacity over others.

Table 4: Objective Analysis of the Pproposed Method

Images	MSE	PSNR	EC (in bits)
Lena	1.7689	45.6551	11532
Baboon	2.4208	44.2913	15420
Barbara	2.0688	44.9796	13866
Pepper	1.5492	46.2334	10290
Airplane	1.6128	46.0611	10890

Table 5 shows the comparative analysis of the proposed method with the existing method proposed by Sahil et al. [6] based on the PSNR parameter. The results show that the proposed method achieves better PSNR over the existing method as shown in Figure 6.

Table 5: Comparative Analysis of the Proposed Method with the Existing Method

Images	Sahil et al. [6]	Proposed Method
Lena	45.6022	45.6551
Baboon	44.2373	44.2913
Barbara	44.9301	44.9796
Pepper	46.2254	46.2334
Airplane	45.9598	46.0611

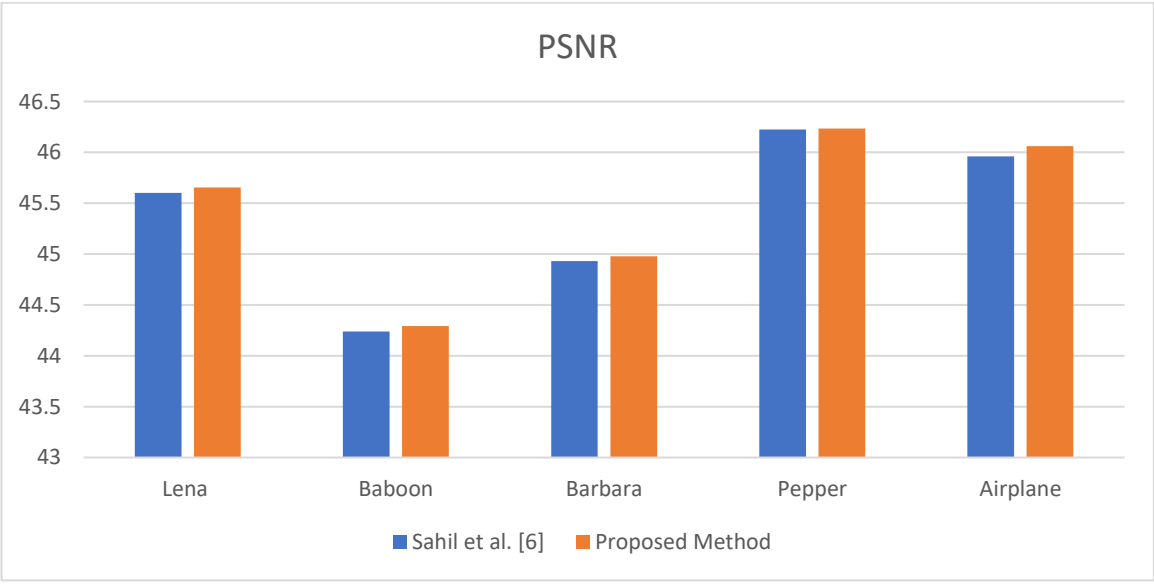

Figure 6: Comparative Analysis based on PSNR Parameter

6. CONCLUSION AND FUTURE SCOPE

In this research paper, we have designed an optimized data hiding method using improved JAYA algorithm for image steganography. In the proposed method, pre-processing on the cover image is done based on HVS characteristics to determine which plane is used for data hiding and which plane is used as reference plane. After that, cover image pixels are split into smooth and edge region using canny edge detection algorithm. The smooth region pixels of the cover images are deployed to match it with secret data bits whereas edge region pixels of the cover images are deployed to hide the optimal matched index using improved JAYA algorithm. The improved JAYA algorithm searches the optimal starting pixels in the edge region pixels. After deteriming the starting pixels, the pixels are hidden in the cover image using 3-bit LSB algorithm. The Performance analysis is done using MSE, PSNR, and embedding capacity parameter. The results show that pepper image achieves the highest PSNR whereas baboon image achieves the lowest PSNR. Besides that, baboon image achieves highest embedding capacity over others. In the last, the proposed method is compared with the existing method proposed by Sahil et al. [6]. The results are superior in terms of PSNR. In the future, the proposed method can be hybridized with cryptography algorithms to achieve multi-layer security.

References

[1] Rehman, A., Saba, T., Mahmood, T., Mehmood, Z., Shah, M. and Anjum, A., 2019. Data hiding technique in steganography for information security using number theory. *Journal of information science*, *45*(6), pp.767-778.

[2] Liu, Y., Liu, S., Wang, Y., Zhao, H. and Liu, S., 2019. Video steganography: A review. *Neurocomputing*, *335*, pp.238-250.

[3] Singh, J., Kaur, G. and Garcha, M.K., 2015. Review of Spatial and Frequency Domain Steganographic Approaches. *International Journal of Engineering Research & Technology (IJERT)*, *4*(06), p.1122.

[4] Shah, P.D. and Bichkar, R.S., 2018. A secure spatial domain image steganography using genetic algorithm and linear congruential generator. In *International Conference on Intelligent Computing and Applications* (pp. 119-129). Springer, Singapore.

[5] Kamil, S., Ayob, M., Abdullah, S.N.H.S. and Ahmad, Z., 2018, November. Optimized data hiding in complemented or non-complemented form in video steganography. In *2018 Cyber Resilience Conference (CRC)* (pp. 1-4). IEEE.

[6] Gupta, S. and Garg, N.K., 2021. Optimized Data Hiding for the Image Steganography Using HVS Characteristics. In *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020* (pp. 275-285). Springer Singapore.

[7] Shah, P.D. and Bichkar, R.S., 2020, June. Genetic Algorithm based Approach to Select Suitable Cover Image for Image Steganography. In *2020 International Conference for Emerging Technology (INCET)* (pp. 1-5). IEEE.

[8] Astuti, E.Z., Setiadi, D.R.I.M., Rachmawanto, E.H., Sari, C.A. and Sarker, M.K., 2020, March. LSB-based bit flipping methods for color image steganography. In *Journal of Physics: Conference Series* (Vol. 1501, No. 1, p. 012019). IOP Publishing.

[9] Abdel Raouf, A., 2021. A new data hiding approach for image steganography based on visual color sensitivity. *Multimedia Tools and Applications*, pp.1-25.

[10] El-Ashmawi, W.H., Ali, A.F. and Slowik, A., 2020. An improved jaya algorithm with a modified swap operator for solving team formation problem. *Soft Computing*, *24*, pp.16627-16641.

[11] Neeta, D., Snehal, K. and Jacobs, D., 2006, December. Implementation of LSB steganography and its evaluation for various bits. In *2006 1st international conference on digital information management* (pp. 173-178). IEEE.

[12] sipi.usc.edu. (n.d.). *SIPI Image Database*. [online] Available at: https://sipi.usc.edu/database/.

[13] Kumar, S. and Singh, B.K., 2021. Entropy based spatial domain image watermarking and its performance analysis. *Multimedia Tools and Applications*, *80*(6), pp.9315-9331.

[14] Pradhan, A., Sahu, A.K., Swain, G. and Sekhar, K.R., 2016, May. Performance evaluation parameters of image steganography techniques. In *2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)* (pp. 1-8). IEEE.

[15] Kanan, H.R. and Nazeri, B., 2014. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert systems with applications*, *41*(14), pp.6123-6130.