Abstract: Steganography is a useful tool that helps to achieve secret communication. Till now the available methods hide the secret data over the image on a fixed pattern that makes a user identify the pattern easily. We are providing a dynamic pattern extraction approach using biometric. According to it some biometric operation detects the edges will be detected we will use this area as the pattern to hide the data over the image. The secret data is compressed using the DWT technique and then further compressed secret information is encrypted using RSA algorithm with bit shift method. This proposed technique provides more security to the data.

Keywords: Steganography, steganalysis, RSA, PSNR, MSE, cover-image, stego-image, DWT, edge detection.

I. INTRODUCTION

Steganography, derived from Greek, means “covered writing”. Steganography is a technique that embedding the secret information into another image so that unknown user cannot identify that secret information [1]. Throughout history, steganography is used for secret transformation of information amongst the public. During Second World War, invisible ink was used to write the secret information on the paper so that the paper appears to an average person as just a blank piece of paper. Liquids such as milk, vinegar, fruit juices were used to read the message. In Ancient Greece, they shave the head of the messenger to hide the secret information at its head and then wait to grow up the hairs and after that the information is extracted by again shave the head of the messenger at the destination site.

Steganalysis: The term steganalysis is basically an art and science which detect hidden secret message using steganography. It is similar to cryptanalysis applied to cryptography. Goal of steganalysis is to identify the packages, detect either there is any encoded message or not, if occurs then recover that message.

II. LITERATURE REVIEW

In today’s world of high technology, it is not safe to share confidential and important data on any network. Intruders are always in wake of it. So, in order to provide strong security, either cryptography or steganography alone is not enough. To keep data secure, the data structure should first be altered before hiding it behind an image. Image steganography is the most frequently used technique of steganography [2]. For hiding information inside images usually Least Significant Bit (LSB) method is used [3]. In this method, the 8th bit of every byte of the carrier file is substituted by one bit of the secret information.

III. PROBLEM FORMATION AND METHODOLOGY

In this paper, the term steganography with proposed methodology is used which enhance the image quality as well as the security of the hidden message. Successful face localization algorithms for color images exploit the fact that human skin tone can be localized within a certain range in the transform color domain (i.e., RGB to YCbCr). Steganography can help from this in such a way that permits us to track and embed into the edge of sequential appearances of human skin in the frames. Human skin tone values, also adjusted within the permissible value ranges, to embed secret data without introducing artifacts on the carrier image.

Problem Definition: As the steganography technique and cryptography technique are information security techniques so that confidential and private data can be protected against unintended access. Both these techniques have their own advantages and disadvantages. Cryptography is having a major limitation that is the existence of data is not hidden. Data that has been encrypted, still present as data. If given sufficient time, somebody could ultimately decrypt the data. This makes cryptography in some way weak and attacks prone. Steganography fails when an unintended person deceits that there is a secret message present in the steganography medium. So a more secure and robust method of communication is required so that confidential and private information is not directly accessible to the otherwise illegitimate person. Now the solution is to have a system that can have advantages of both that is the data is encrypted as well as steganographed. Two factors are used to measure the quality of stego image

a) PSNR (Peak Signal to Noise Ratio).

b) MSE (Mean Square Error).

Greater the PSNR value indicates the higher quality of Stego image.
Objective and Scope: The main objective of this work is to improve quality of the Stego image and provide security to the secret image by RSA encryption with bit shift method. The algorithm is implemented on MATLAB and the quality of the image is analyzed on the basis of PSNR and MSE values. The quality of the image must not be distorted after hiding the data in it so that the presence of the image is not recognized to human eye. For this to be achieved PSNR of the stego image to cover image must be high and the MSE must be low. The research methodology is as follows:

1. Refer various journals, research papers and books for attaining adequate knowledge in steganography. Obtain a profound understanding of image steganography.
2. Select a subtype of steganography to work upon. This research work focuses on image steganography.
3. Propose an algorithm that will be the basis of future work.
4. Select a tool that will be used to implement the proposed algorithm.
5. Implement the algorithm and analyze the results.
6. Compare these results with previous algorithms [4].

IV. IMPLEMENTATION

To implement the algorithm, first the cover image is loaded and then skin tone detection is done when the cover image is biometric and if the image is non-biometric then edge detection algorithm is applied. After that the secret image is loaded and DWT method is applied to it which will give compressed secret image. Then encryption is done using the RSA with bit shift method. Encrypted image is then embedding into the edge pixels of the cover image. This method of data hiding is more secure as secret image only uses the edge pixels and data is not dispersed in the whole cover image. As distortion of cover image is less and then the image quality of stego image is good.

Proposed Algorithm

As there are various steps to implement the steganography here.

1: Cover image is loaded & skin color detection is done for the biometric image.
2: Apply canny edge detector algorithm for the image.
3: Once the edges detected then load the secret image.
4: After loading the secret image, DWT technique is applied to compress the secret image as compressed image will less distort the cover image.
5: Then RSA encryption algorithm with bit shift method is performed.
6: Encrypted message is then embedded behind the cover image.
7: Stego image with better quality is obtained.

All the above steps are followed to hide the secret data over the cover image. The correlation property is exploited in a proposed technique [5].

Flowchart

The flowchart represents the method of hide data by the proposed framework.

**Parameters Used (MSE and PSNR):**

Detecting an embedded message defeats the primary goal of steganography, that of concealing the existence of a hidden message. As steganography is based on obscurity, the most important tests are related to the human perception. These types of tests evaluate the invisibility or transparency. The most used tests are the Subjective and the Peak-Signal to Noise-Ratio PSNR in decibel. The skewed tests are taken out by people who look for visual differences between the images (original and stego image) trying to find which one of them is the original. If the percentage of success goes 50%, it can be concluded that the message is invisible. The test rules commendations are defined by the International Telecommunication Union (ITU). Unlike the subjective approach which is vulnerable to human vision, PSNR (Peak Signal to Noise Ratio) is a technical approach usually used to evaluate the real quality of stego image [6]. This technique is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The PSNR is most commonly used to...
measure the quality of reconstruction in an image; by comparing the stego image with the original image. PSNR can be calculated using the mathematical models/formulas in Equations below. First MSE is calculated using the following equation:

\[ MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \]  

Where MSE is the Mean Squared Error of \( m \times n \) monochrome images \( I \) and \( K \), where one image is considered a noisy approximation of the other, where lower is better. Thereafter, PSNR can be calculated using the following equation:

\[ PSNR = 10 \log_{10} \left( \frac{\text{MAX}}{\text{MSE}} \right) = 20 \log_{10} \left( \frac{\text{MAX}}{\text{MSE}} \right) \]

Where, \( \text{MAX} \) is the maximum pixel value of the image.

**Experimental Results**

DWT algorithm and RSA algorithm with bit shift method was implemented and executed using MATLAB. The cover and stego images are compared on the basis of MSE and PSNR. PSNR and MSE are the most commonly used metrics for measuring the quality of stego image. The experimental results convey that this technique provides sufficiently good PSNR value.

Figure 5.1 and Figure 5.2 represents YCbCr Color Space Images and Skin detection and Edge detection of the Cover Image. As first the cover image is loaded and then skin pixels are evaluated. After the Evaluation of skin pixels, edge detection algorithm is performed by using the canny method as this method hide the secret data only in the edge pixels which provide more security.

Figure 5.3 Secret Image Which is Hiding Behind the Cover Image

Figure 5.4 Decomposition by DWT

Figure 5.3 and Figure 5.4 represents Secret Image which is hiding behind the Cover image and Decomposition of secret image by DWT method. After performing the edge detection, the secret image is loaded and DWT technique is applied at the secret image.

Figure 5.5 Compressed Secret Image
Figure 5.5 represents compressed secret image. As this image is encrypted and hide behind the edge pixels of the Cover image.

![Original Image and Stego Image](image)

Figure 5.6 Image1 Original Image and Stego Image

Figure 5.6 represents Image1 showing original and Stego image. Secret image is hiding behind the cover image and their parameters are calculated:

Obtained values of the parameters are:

PSNR= +33.667 dB. Time Taken = 2.953.

![Original Image and Stego Image](image)

Figure 5.7 Image2 Showing Original and Stego Image

Figure 5.7 represents Image2 showing original and Stego image and their parameters are calculated:

Obtained values of the parameters are:

PSNR= +34.667 dB. Time Taken = 4.187.

<table>
<thead>
<tr>
<th>Cover Images</th>
<th>Secret Images</th>
<th>PSNR Value By LSB Method</th>
<th>PSNR Value By Proposed Algo</th>
<th>Time Taken (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1</td>
<td>Flowr.jpg</td>
<td>30</td>
<td>33.667</td>
<td>2.953</td>
</tr>
<tr>
<td>Image2</td>
<td>Rose.jpg</td>
<td>29</td>
<td>34.083</td>
<td>4.187</td>
</tr>
<tr>
<td>Image3</td>
<td>Child.jpg</td>
<td>32</td>
<td>37.864</td>
<td>3.108</td>
</tr>
<tr>
<td>Image4</td>
<td>Teddy.jpg</td>
<td>30</td>
<td>34.083</td>
<td>3.046</td>
</tr>
</tbody>
</table>

Table 5.1. Experimental Results

The above table shows the experimental Results of the proposed algorithm. PSNR values obtained by the proposed algorithm are better than the existing LSB method.

VI. CONCLUSION AND FUTURE WORK

As steganography is concerned with security purpose. The proposed algorithm pre-processes the data before hiding it behind the cover image. The compression step taken in the algorithm reduces the size of text and thus allows more data to be hidden behind the image. The skin area and the edge pixels are evaluated and secret data which is encrypted with RSA algorithm is embedded into specific area. As data is embedded in certain region rather than whole image so security as well as quality of stego image is enhanced. The data is secreted only in the edge pixels of cover image which is least imperceptible to human eye thus providing a higher PSNR value and no visual distortion of image quality. Moreover, the size of the image does not change after hiding the text in it.

In future, this technique may be modified by pre-processing the data in a different way. A different compression algorithm like DCT (Discrete Cosine Transform), Vector Quantization, Huffman coding can be used according to the efficiency required. For data encryption different algorithms like AES, DES can be used for more security. For example, it can be used in fields like e-commerce, and the transport of sensitive data.

VII. REFERENCES


