**Abstract**

Steganography is the idea of hiding sensitive data within some media like text, audio, video, or image that appears to be nothing out of the normal. The key issue in image steganography is having high embedding capacity and capability to withstand against stego attack. Researchers in this field are still looking forward to increasing the amount of the capacity while having a maintained image quality. In this paper First a compression technique is applied on the secret message in order to minimize size of the secret data that needs to be embedded into the cover image which leads to increase the embedding capacity then in order to hides the data a combination of two algorithms are used. First In order to achieve more security and we use p-Fibonacci series technique to decide which pixels will be used to embed the secret digits. second in order to achieve more capacity and maintain high PSNR we use modulus function to hides data which depends on convert the secret message from ASCI to r-base-r:2,3,4,5…etc- so that instead of embedding 8 digits for each character we can embed only 4 digits if we use r=4 -for example. The time of the embedding and extracting processes is one of steganography issues because of that we use parallel programming techniques to minimize the time consuming.

***Keywords—Steganography, Protecting data, information security, information hiding, pixel value modification, modulus function, Fibonacci, Security.***

**Previous methods**

1. Pixel Value Modification Method using Modulus Function

In 2013, Nagaraj et al. [15] introduced a pixel value modification method using modulus function. Their method divides colored cover image into three planes (or components) namely, Red, Green and Blue where every pixel contains 24 bits (8 bits for each color). Additionally, in this method, all three components have been used for data embedding after applying modulus three function to the pixel values in each color component. Their embedding process is explained by following steps: Step 1: Separate the color image into three components color matrices and apply the next steps on each of them sequentially i.e. apply the next steps on the first pixel value of Red matrix, Green matrix and the first pixel of the Blue matrix. The same process continues for the second pixel value of each plane until all pixels are accessed. Step 2: Let ܵ be the secret digits in base 10. These digits are first converted into base 3 values after that the obtained digits are embedded into three planes. Step 3: Pixel values are grouped into different sets (red,grean,blue) with these three parameters representing the set for Red, Green and Blue pixel values respectively. Step 4: The suitable pixel to be selected for embedding should fall in the range of 0<gi<255. Step 5: Perform the embedding by increasing or decreasing the original pixel value by ͳ or െͳ respectively. Note that the decision for embedding data is taken after comparing the modulus values and the digits to be concealed. That is, having the secret digits ܵ and the values obtained by applying modulus three function on each pixel value which are denoted by .During the extraction, the stego image is divided into three planes Red, Green and Blue correspondingly after that the secret digits are obtained by applying modulus three function to each pixel value. Moreover, the extracted digits values have to be converted back to base 10 to get the original secret message.

1. Enhanced PVM

In 2017 an enhanced method discussed can handle any modulus function, i.e., the limitations encountered in the previous method are completely removed. This allows one digit of the secret data to be concealed in each pixel. Moreover, the effect of varying modulus function is also analyzed. The experiment shows that the suggested enhanced-PVM does achieve good performance. Besides, good embedding capacity and PSNR are achieved while using modulus 2, 3 and 4. On the other hand, for modulus 5, 6 and more, the embedding capacity changes slightly.

C.An Intelligent Fibonacci Approach

First, a key is passed using an algorithm such as Diffie-Hellman. This key is divided by 10 to get a single digit remainder, say x. x is then used to determine which pixel value is going to be modulated. x is passed as the parameter to a Fibonacci p-code number system. The output obtained say m is taken as the first pixel to be modulated, afterwards all multiples of m such as 2m, 3m etc are modulated. Once all the multiples of m are completed, the last multiple is taken and divided by 10 and the process is repeated till complete data is hidden.

PROPOSED ALGORITHM

Our algorithms depends on a combination of two algorithms, the first is use the Pixel Value Modification Method using Modulus Function to hiding the secret data, the second is the pixel location choosing for hiding data using the p-Fibonacci series method .

The first method[] modifies the image pixels in order, which make the security of the algorithm very low and the second method using lsb to embedding the data which give low capacity, our algorithm merge the previous two methods in order to overcome their limitation the p-Fibonacci make our algorithm strong and secure enough and the pixel modification algorithm increases the capacity.

We also using parallel programming to decrease the time consumed by the algorithm.

A. Steps for Performing the Embedding

**Step1**:Obtain the secret message (msg) and apply compression algorithm on the message in order to minimize number of bits which will embeds in the cover Image.

**Step2**:Divide the cover image into 3 channel imgR, imgG, imgB.

**Step3**:Using p-Fibonacci to generate key position list for each channel

**Step4**:Divide the message into blocks

**Step5**:Create number of threads each thread will embeds one block of the message using pixel modification algorithm

**Step6**:Finally we have to embed the message length in the cover image in order to extract the original message.

**B**. Steps for Performing the Extracting

**Step1:**extract the length of the secret message from the image.

**Step2:**Divide the stego-image into 3 channel imgR, imgG, imgB.

**Step3:**Using p-Fibonacci to obtain the key position list for each channel.

**Step4:**Extract the secret message bits from specified positions using pixel modification algorithm.

**Step5:**decompress the obtained message.

IV. EXPERIMENTAL RESULTS

The proposed system was tested against PSNR Value with respect to the modulus function being applied and the size of secret message with different cover images . The database consisting of the images is the USC-SIPI database [18].Figure 1 shows some images used for testing of the algorithm before and after the execution

Image before embedding  

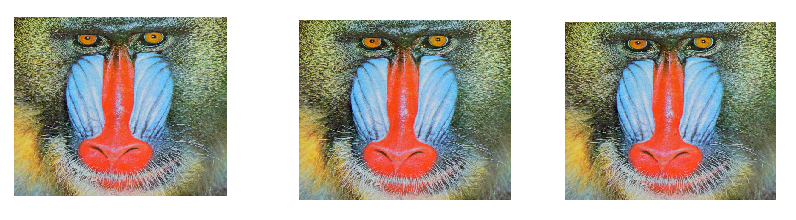

Figuer1 image after embedding Secret message of size 200K using mod 3,5,7 respectively.

Image before embedding

Figuer2 image after embedding Secret message of size 100K using mod 3,5,7 respectively.

TABLE I. PSNR VALUES DEPENDING ON THE SIZE OF THE SECRET MESSAGE WITH MODULO 4