ISSN: 0976-3104

SPECIAL ISSUE (SCMDSA)

ARTICLE OPEN ACCESS

A NOVEL RGB BASED STEGANOGRAPHY USING PRIME COMPONENT ALTERATION TECHNIQUE

Anil Sathyan*, Mythili Thirugnanam, Sumit Hazra

[12,3] *School of Computing Science and Engineering, VIT University, Vellore, INDIA*

ABSTRACT

Steganography is the science with the help of which secret or confidential data is hidden within any media like text, images, audio or video and protocol-based network. As privacy concerns continue to develop, it is in widespread use because it enables to hide the secret data in cover images. Steganographic techniques are best suited for digital image processing. In general, Steganography is classified into spatial and transform domain techniques. This paper presents a new RGB based algorithm in spatial domain called Prime Pixel Alternation technique. In the present scenario, many spatial domain algorithms like LSB, first component alternate, pixel indicator are usually used for steganography since they are easier to implement and less complex. Even though their hiding capacity is high, they are more prone to steganalysis. A new RGB-based algorithm is designed to store data in Random prime numbered multiple pixel locations and the encrypted key is also stored along with the data in a co-prime location (co-prime to the aforesaid 3 numbers).This algorithm requires to choose 3 random numbers to store data in R(Red), G(Green) and B(Blue) components of the cover image(24 bit image).Blue component is given the priority to store more data (lowest prime no: multiple pixel location) because a research was conducted by Hecht [14], which reveals that the blue objects ,if visually perceived , are intense and are comparatively less distinct than the red and green objects . Since the key size is fixed, it is stored in co-prime pixel locations, which will be least in number. Key bits will be stored in R, G, B components one at a time in a cyclic manner, in the above mentioned co-prime locations, in which the security is improved. A null terminator bit pattern may be used to indicate end of key or data. The reverse process of the encoding algorithm is used to decode the message.

Received on: 30th-November-2015
Revised on: 22nd-February-2016
Accepted on: 12th–February-2016
Published on: 16th–May-2016

KEY WORDS

Steganography; RGB; First Component Alternate; LSB; Steganalysis.

***Corresponding author:** **Email:** anil.sathyan2015@vit.ac.in; **Tel.:** +91-416 - 2202000; **Fax:** +91-416-2202041

INTRODUCTION

Due to rapid advancement in the fields of both computer technology and the internet one of the most essential and important factors is the communication over the internet which requires security and authenticity of information and thus that of the users as well. For exhibiting the mechanisms for the security of data transfer to and fro over internet either of the two mechanisms can be adopted which are namely Cryptography and Steganography. The art of hiding information is known as Cryptography (which is a Greek word with basically two components: kryptos (meaning hidden) and logos (meaning word).The main and ultimate goal of cryptography is user authentication, data authentication and data confidentiality. Steganography just adds another level of security to it. It basically involves the composing of messages so that only the sender and the receiver only knows that the message even exists thus avoiding any unwanted third-party attention and hence no possibilities for their intrusion. Mainly it is of three categories : Steganography in image , Steganography in audio iii) Steganography in video and in recent literature Steganography in text has also been proposed. Steganography for image and text has been worked upon. The general classification of Steganography is shown below in **Figure– 1.**

Some of the applications of our technique are being described in this paragraph. It can be used in the corporate world for transmission of confidential data without any third-party interception. It is also used in business for hiding any of the ideas or plans for a new invention. The simplest and the oldest application is that in map making where cryptographers sometimes add a tiny fictional street to their maps, which allows them to track and hence prosecute copycats. Photo collections which are sold on CD , often have hidden images in the photos which allow detection of unauthorized use. When the same technique is applied to DVDs it is even more effective and useful, as the industry builds DVD recorders to detect and at the same time disallow copying of protected DVDs and thus preventing unauthorized use. Four essential parameters for the evaluation and analysis of the quality of a Steganographic algorithm are : Imperceptibility, High data hiding capacity, Security and Robustness. In this proposed algorithm parameters such as imperceptibility, data hiding capacity and security has been focused upon mainly.Thus , through our proposed algorithm we are basically ensuring an advanced level of security by including symmetric key based

THE IIOAB JOURNAL
ISSN: 0976-3104

encryption technique and at the same time maintaining a perfect balance between other steganographic parameters as mentioned above, thus optimizing the algorithm . Some of the related works done on this topic are briefly discussed in the following sections.

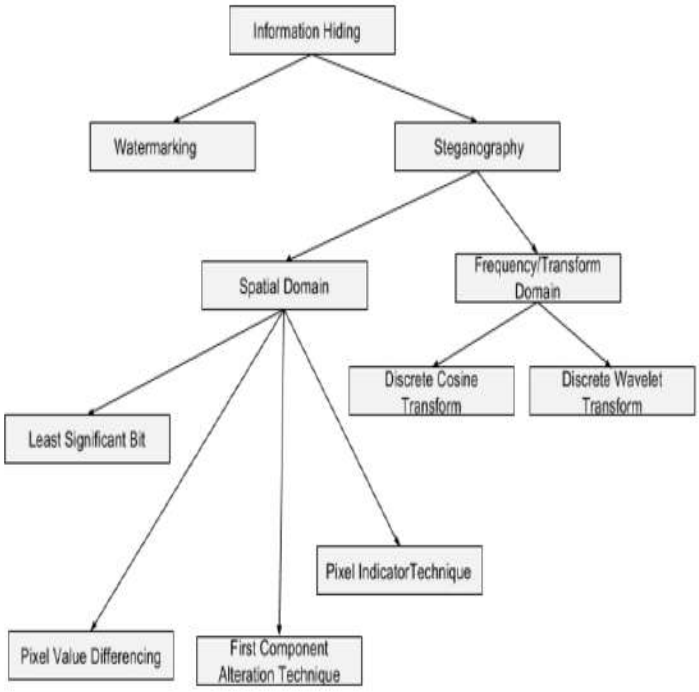

Fig: 1. Steganography Classification

MATERIALS AND METHODS

Basic Techniques and Related Works

Least Significant Bit (LSB) Data Hiding Technique

This method is the easiest way of hiding information may it be in the form of text or image in a cover image. In this very technique, the Least Significant Bits (LSB's) of the pixels are considered individually at a time which further undergoes replacement with the message that is to be sent, in which each bit of the message is hidden in each LSB. The message bits are permuted before the task of embedding is performed, which distributes the bits in an even manner, thus on an average only half of the LSB's will be altered or modified. Using this concept Darshan R., R Prabhu et al. **Error! Reference source not found.** have proposed a Steganographic technique in which though the code for Steganographic technique is easier to implement ; the statistical methods for Steganalysis makes it all the more insecure and is vulnerable to corruption.

Pixel Value Differencing (PVD) Technique

The alteration of edge areas in the visual system of human beings cannot be distinctly recognized separately or distinguished well, but if the small areas are altered such alterations can be well identified with distinguishing features. So more confidential and secret data can be hidden in an edge area than a smoother one. With this concept, Yang, Cheng-Hsing et al. [13]through a paper have put forth a Steganographic scheme in which they have used combined methodologies of Adaptive LSB and Pixel Value Differencing. Though this paper gives high adaptability, capacity, image quality and imperceptibility but then pixel value is varied from 0-255 which is a major disadvantage besides data is hidden along edges only, thus giving a lower embedding rate overall.

First Component Alteration Technique

Many Steganographic schemes are existing but a new advanced spatial domain Steganographic scheme which is the First Component Alteration Technique is being discussed here . The First Component Alteration technique is used to hide secret data or image within the cover-image which is comparatively bigger. Focus is mainly on the two bits or the four bits of a pixel in a image with

THE IIOAB JOURNAL ISSN: 0976-3104

a maximum of five bits at the edge of an image which results in less PSNR(Peak Signal to Noise Ratio) and a high value of root mean square error. The technique uses 8 bits of blue components (as in RGB (Red, Green and Blue) where Blue is considered the First component of pixels are replaced with secret data bits one by one in the proper sequence. This scheme can hide more data than previous schemes and give a better image quality but then it cannot be applied for those images which have less blue component ,which is its major disadvantage. With this concept Kaur, Amanpreet et al. **Error! Reference source not found.** have proposed a random 8-bit alteration technique for Steganography which though provides a higher data hiding capacity, imperceptibility and better image quality but cannot be applied for those images which have a lesser blue component.

Pixel Indicator Technique

Image based Steganography basically is based upon the fact that the images are utilized as cover media to hide confidential data. The common technique that has been used replaces the LSB bits of the image pixels with the intended secret bits. Several efforts to improve the security of the LSB method have already been emphasized through earlier presentations. This paper has proposed an enhanced technique which utilizes the 24 bits in each pixel in the RGB images by using the two least significant bits of one of the channels to act as an indicator for the existence of data in the remaining two channels (R/G/B). This Steganographic method does not use a separate key to remove the overhead of the key management. Instead, it is using the secret data size as the main criteria for selection of the first indicator channel to insert security and randomness. Our proposed technique has been compared with two other similar works by analyzing the security and capacity of respective techniques. This pixel indicator technique for RGB images has showed better results compared to previous techniques.

In prior studies, one of the most popular and the oldest techniques for Steganographic Data Hiding has been the LSB mechanism in which the data bits has been embedded by substituting the Least Significant Bits of the binary representations of the RGB components of each pixel. According to the study conducted by Darshan R et al. [3] the LSB substitution technique's GPU execution is 20 times faster and even easier to implement. However, a statistical method for Steganalysis makes it insecure and thus making it vulnerable to corruption. A similar study carried out by Kaur et al. [11]focuses on the First Component Alteration Technique. Here, they embed the data bits into the blue component only thus having a higher data hiding capacity, imperceptibility and better image quality, yet it fails its application for those images which have less blue component. In another case Bharti et al. [4] adds another layer of security to the existing techniques and imperceptibility by using Vigenere Cipher; but it is having a primary weakness which is the principle of the repeating key. In another notified paper by Mahimah et al.[5] the same Steganographic technique has been utilized by using a new and different approach that is of a Zigzag Pixel Indicator Technique which gives us a high quality stego image providing better security than the existing LSB techniques. But, on the other side it is computationally complex and has high space requirements. A paper on Steganography by M.G.Gouthamanaath et.al uses the concepts of Pixel Value Differencing (PVD) and Pixel Indicator Technique (PIT)[1] which reduces the existing computational costs and provides a good image quality; yet in their paper the hidden capacity depends on Cover image pixel intensities. In another important paper by Luo et al. [12]the Steganographic analysis uses the techniques of Edge Adaptive Image Steganographic scheme in Spatial Domain LSB where data is hidden adaptively only in the specific edges. Even though the technique used, preserves the statistical and visual features its embedding rate is sufficiently low. But again the aforesaid technique can be extended to audio/video Steganography. Delving into the world of Steganalysis a related paper by Fillatre et al. [7] focuses on the Statistical Hypothesis Testing for the LSB mechanism which maximizes the probability of detection; yet the technique used is the LSB technique but with increased number of assumptions and also requires hiding of extra bits of signature with hidden message .

Most of the research carried out uses LSB (Least Significant Bit) Technique for embedding the data bits with improved security and imperceptibility yet, images of higher resolutions are required which is mostly covered by our research. With these intentions this work involves an algorithm which aims for a better data hiding capacity and improved security since it uses encryption techniques along with Steganography, thus also making the technique more robust. Focus is basically on the spatial domain as the pixels can directly be manipulated , but in contrast to it is the Transform Domain in which the process has complex transformations in the very specific frequency domain. Even though the Transform Domain technique is less susceptible to external interference e.g. Noise or Corruption but then it has less data hiding capacity when it is compared to Spatial Domain which is basically the platform under consideration. Thus the aim is to achieve a perfect balance between Imperceptibility, Data Hiding Capacity and Security through the proposed methodology that follows.

Proposed Work

The proposed Steganographic algorithm is basically a RGB-based prime-pixel alteration technique .Our Steganography is applicable for both images and texts respectively. At first a message (either an image or a text)is being taken as an input .The message is encrypted with the key and only after its proper encryption the message is embedded in the cover image. Basically to describe explicitly the process involves saving each of the data (text or input image converted into strings) bits in the prime pixel locations of the Red, Green and Blue Components' groups of 3 random numbers or prime triplets. And since the key is of a fixed size the key bits are stored in co-prime pixel locations. The key bits will be stored in the Red, Green and Blue components one at a time in a cyclic manner for enhanced security. For storing the data, the Red, Blue and Green components are basically being considered. For decryption or decoding the original message with quality fully retained and without any third party interception, the reverse process of the encryption algorithm has been followed. This can be better understood through the block diagram described below.

The basic functional block diagram of the proposed method is shown in **Figure– 2**. Firstly the payload data(image or text) is encrypted before embedding. Then, the key along with the encrypted message is embedded using the proposed technique larger

ISSN: 0976-3104

cover images are chosen for better hiding capacity. The resulting stego-file is transmitted via any communication channel to the intended receiver. At the receiving end the receiver extracts the key from stego file with the help of shared secret data(prime triplets). Using the key the extracted information is decrypted to get back the original message. The cover image is obtained as a byproduct. The complete embedding and extraction algorithms are fully described below with the help of flow diagrams in the following sections.This schematic diagram provides an outline of the basic working of the stegnographic technique.The implementation can be done in different ways depending on the types of encryption, data type, media etc.

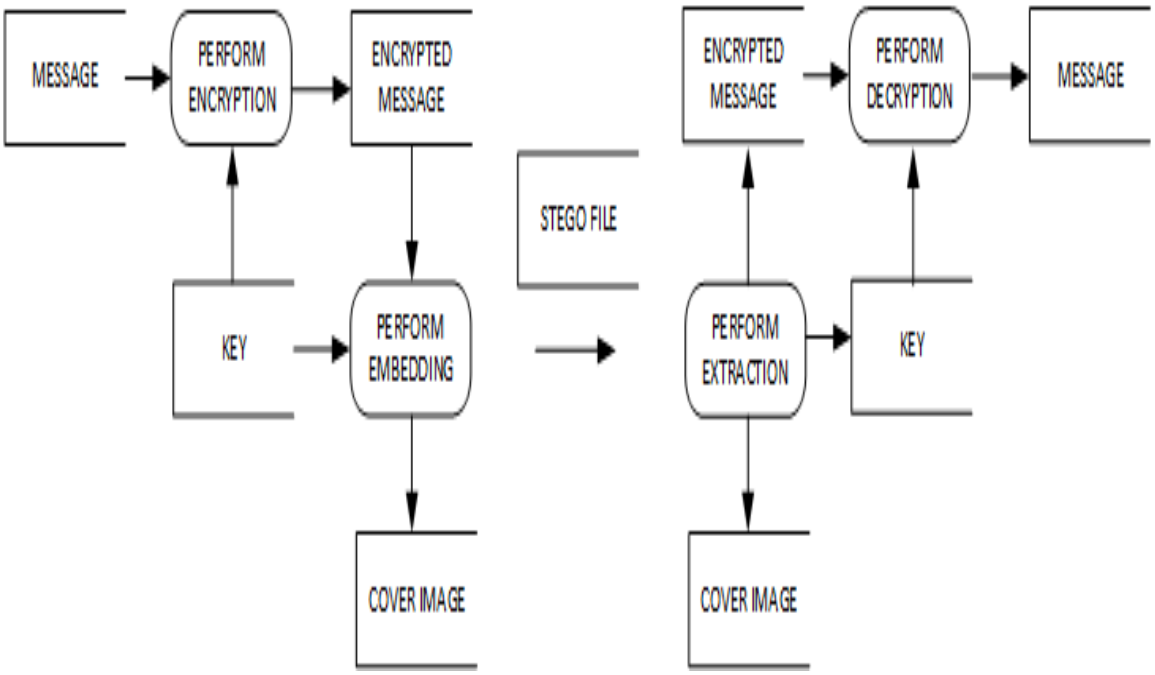

Fig: 2. Schematic Diagram

……..

The detailed flow diagram of the embedding and extraction phases of the algorithm are discussed in the following sections. The extraction algorithm is almost the reverse process of embedding. The entire process can be depicted in the form of flow diagrams as shown below.

Algorithm

The algorithm has two phases namely Embedding and Extraction. The detailed description of Embedding and the Extraction phases with the use-case scenario is described below:-

Person A wants to send a secret file (image or text file) to Person B through a insecure channel. Person C is an intruder who as access to the covert channel information. Person A and B has shared information about a prime triplet, which will be used as an input in this algorithm. Person A uses a large image to hide his secret data and a random 24 bit key.

THE IIOAB JOURNAL
ISSN: 0976-3104

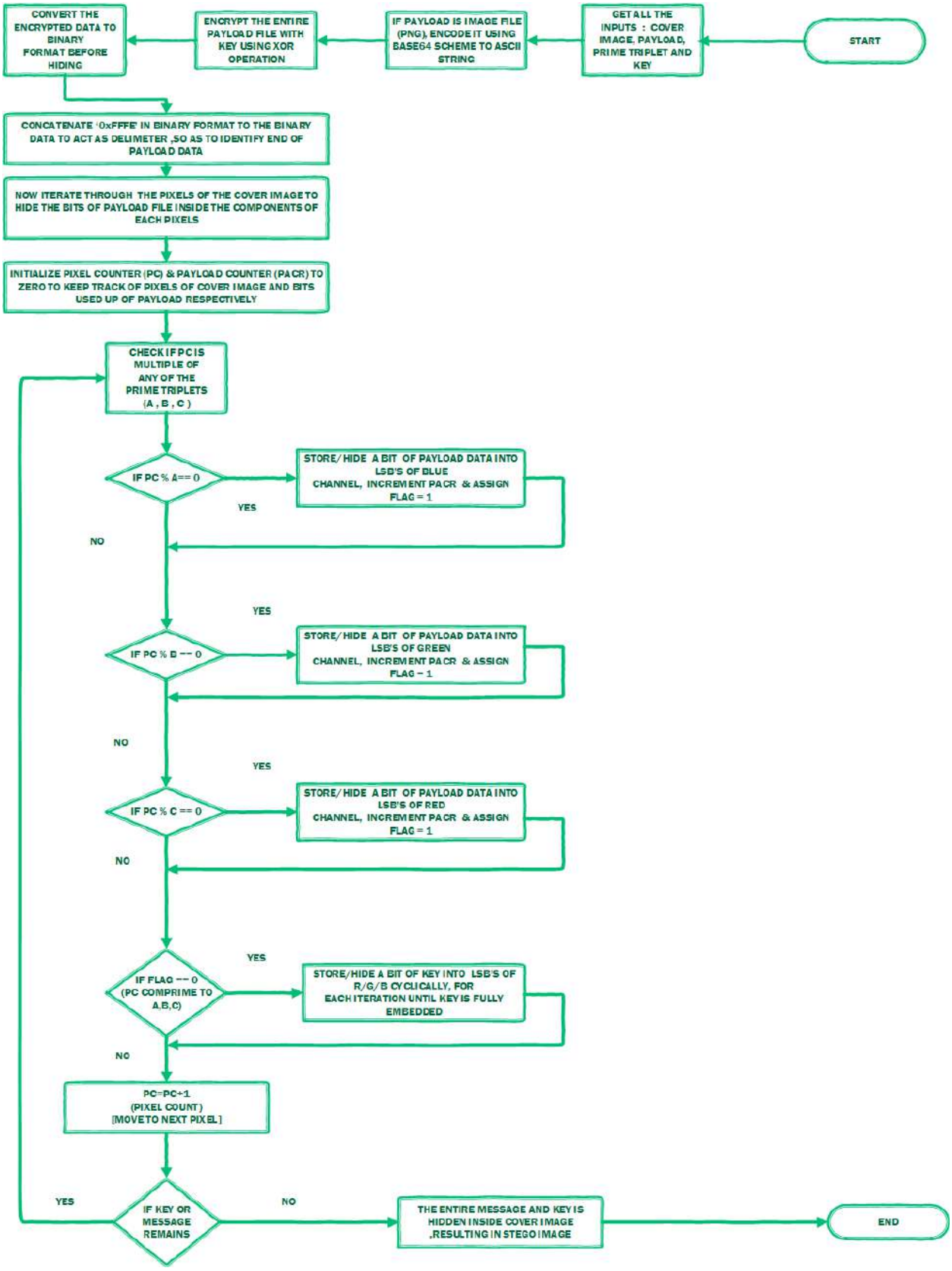

Fig: 3. Embedding Process

……

THE IIOAB JOURNAL
ISSN: 0976-3104

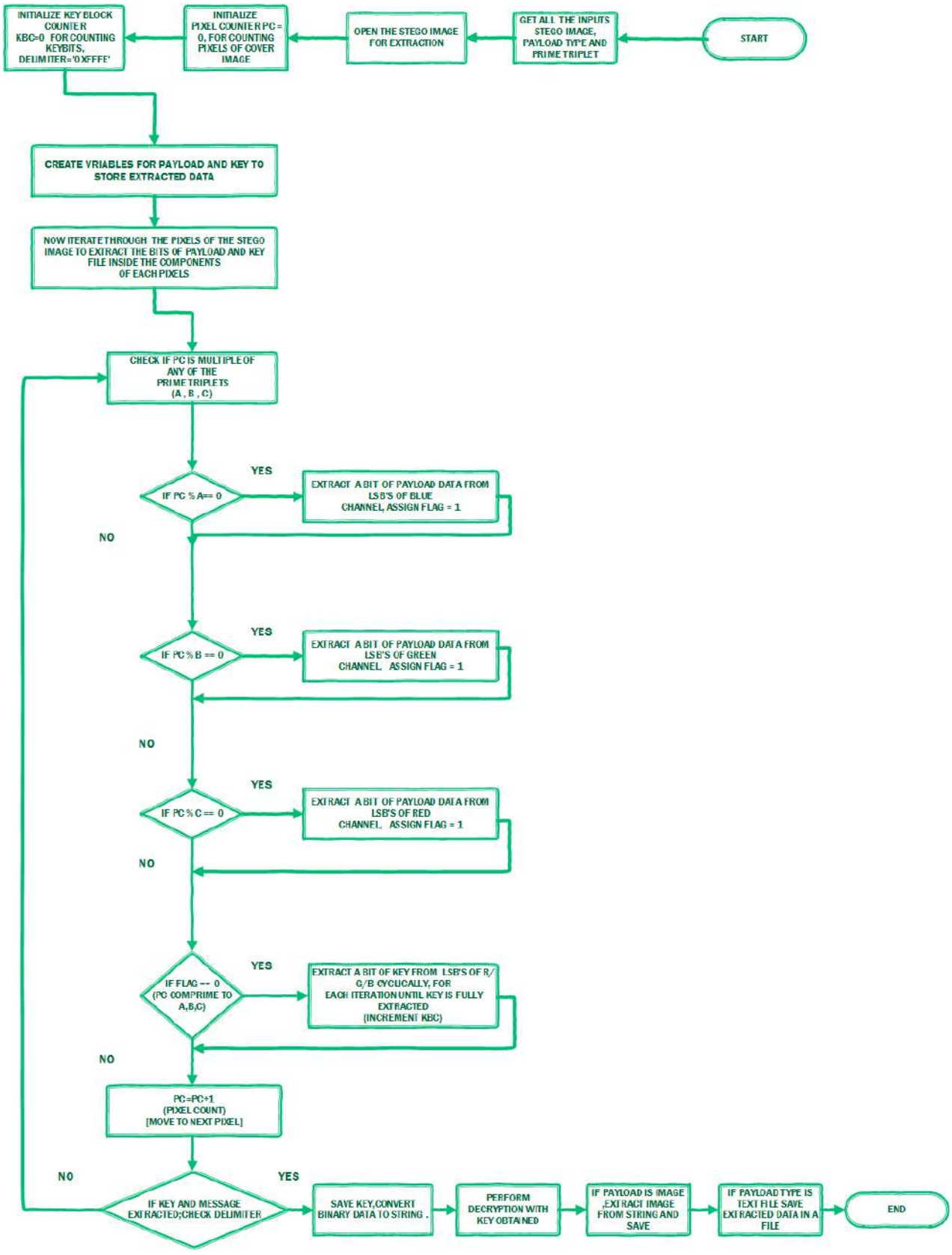

Fig: 4. Extraction Process

……

THE IIOAB JOURNAL
ISSN: 0976-3104

Steps followed for ***EMBEDDING***:

INPUT: {COVER IMAGE, SECRET FILE (PAYLOAD), KEY (24 BIT), PRIME TRIPLET (P1, P2, P3)}
OUTPUT*:* {STEGO IMAGE}

1. Get all the inputs and check the payload type, whether it is an image or text file.
2. If it is an image (PNG), encode it using base64 encoding scheme to an ASCII string else, do not encode the data.
3. Now encrypt the string using XOR with the key, with the help of standard library functions to get encrypted data.
4. Convert the encrypted message to binary string
5. Add a delimiter string '0xFFFE' to end of the binary data obtained, so as to identify the end of the payload data.
6. Now open the cover image and iterate through the pixels of the image
7. Initialize the pixel counter PC = 0 payload counter PACR = 0, and for each pixel in the cover image do the following until the entire payload and key is embedded

7.1. If PC is multiple of P1 then replace LSB's of the BLUE component by the bits of the payload binary data. Increment payload
counter accordingly.
7.2. If PC is multiple of P2, then replace LSB's of the GREEN component by the bits of the payload binary data. Increment payload
counter accordingly.
7.3. If PC is multiple of P3, then replace LSB's of the RED component by the bits of the payload binary data. Increment payload counter accor-
dingly.
7.4. If PC is NOT multiple of P1, P2, P3, then replace LSB's of the R/G/B component by the bits of binary key string ,cyclically in each
iteration (one component at a time).
8. After each pixel is saved, save this stego image in the required format (PNG).
9. If payload size exceeds capacity, throw error.

If Person B receives this cover image, he can get back the secret data from cover image, by using the extraction algorithm (reverse process), provided he has the shared prime triplet information..The key is embedded within the cover image.

Steps followed for ***EXTRACTION:***

INPUT: {STEGO IMAGE, PRIME TRIPLET (P1, P2, P3)}
OUTPUT: {COVER IMAGE, SECRET FILE (PAYLOAD), KEY (24BIT),}

1. Get all inputs, Use delimiter='0xFFFE' for checking end of message.
2. Get payload type from user that is image or text.
3. Open stego image, initialize the pixel count PC = 0, for iterating through pixels of stego image; Create variables payload,
key(empty initially for storing the corresponding bits during extraction process.
4. While the payload data is not completely extracted do the following by iterating stego pixels, use the delimiter to check for end
of data.
4.1. If PC is multiple of P1, then extract LSB's of the BLUE component and add it to the bits of the payload binary data.
4.2. If PC is multiple of P2, then extract LSB's of the GREEN component and add it to the bits
of the payload binary data.
4.3. If PC is multiple of P3, then extract LSB's of the RED component and add it to the bits of the payload binary data.
4.4. If PC is NOT multiple of P1, P2, P3, then it to extract LSB's of the R/G/B component, addthe bits of binary key string ,cyclically in each
iteration (one component at a time).
5. Save the key for decryption
6. Convert binary data to string.
7. Perform decryption using XOR , with the key obtained.
8. If payload is an image, extract the image from the string and save the image.
9. If the payload is text file, save the extracted as data text in a new file.

Thus the person B can get back the secret data (text/image) from the cover image. But here, the cover image cannot be recovered fully. If the person C (intruder) has no knowledge of the prime triplets, he won't be able to extract the message from the stego image; even though if he somehow hacks the extraction algorithm. The encryption carried out on the secret data serves as an additional layer of security.

THE IIOAB JOURNAL
ISSN: 0976-3104

Module Description

The input of the algorithm consists of a large cover image, secret data (image/text), 24 bit key and a prime triplet. The key size is selected to be 24 since an image (png) having RGB format with 24 bits per pixels has been used.

The prime triplets are ordered pairs of form (p1, p2, p3) such that p1<p2<p3 .They are selected randomly and should be very less than size of secret data to be hidden. These numbers are shared between two parties involved in communication. A **prime triplet,** in mathematics, is defined as a set of three prime numbers of the form (p, p + 2, p + 6) or (p, p + 4, p + 6).For example ordered triplets like (5, 7, 11), (7, 11, 13), (11, 13, 17), (13, 17, 19), (17, 19, 23), (37, 41, 43) etc..In our algorithm it can be any 3 random numbers or numbers of the form just mentioned above.

Here the value of each number determines the number pixel components modified. (p1, p2, p3) corresponds to (B, G, R) components respectively. The main process of the algorithm consists of iterating through the pixels of cover image. For this the pixels are numbered sequentially and then check for each pixel if it is a multiple of any of the prime triplets. If it is multiple of p1 hide the bits of secret data in LSB's of BLUE component; if it is multiple of p2 hide the data in GREEN component and finally if it is a multiple of p3 the data is hidden in the RED component of the pixel. Since p1<p2<p3, Blue component is modified most number of times, followed by green and finally Red component is modified least when considering total pixels modified. This is done because a study conducted by Hecht et al.[14] suggested reveals that that the visual perception of blue objects those are intense is comparatively less distinct than that of the perception of objects that are colored red and green.

In this algorithm ,the image is converted into base64 encoded format for easier processing. Then the specific key is used to encrypt the data using XOR operation.XOR operation can provide moderate security as long as key is not compromised. The property of XOR is that once XOR operation is done using a key, the original message is obtained back from cipher text just by performing the same XOR operation with the same key on the cipher text. For example:-

DATA: 10011100 XOR (⊻)
KEY: 01101100
CIPHER: 11110000

KEY: 01101100 XOR (⊻)
CIPHER: 11110000
DATA:10011100

The data is converted to binary format so as to easily embed the same inside the component bits of the pixels. A delimiter '0xFFFE' in binary format is used for identifying the end of message. At each iteration process described above counters are used for the pixels of the cover image and also for the data and key so that the iteration can be stopped when entire key and data is embedded inside the cover image. The key is embedded inside the pixels whose number is co prime to prime triplets. The component positions in which the key bits are hidden (of pixels of the cover image) are changed cyclically. This adds some 'confusion' to the encryption scheme. The main aim of Steganography is to conceal the existence of data inside cover-image. Now by adding additional security, even if the existence of message is found out the hacker will be unable to extract the message in unencrypted form.

The algorithm will have a maximum hiding capacity based on the size of the cover image. Also this will also depend on the selection of the prime triplets. Generally, using a smaller prime triplet one can get higher hiding capacity since data is hidden only in pixel locations which are multiple of the prime triplets. So this prime triplet values can be used for tuning the algorithms hiding capacity, keeping the cover image size constant.
Images in PNG format and text files have been used as payload (secret data) and the performance was as good as expected.
In the extraction phase only the stego-image and prime triplets are required as inputs, since the key is already embedded inside the stego-image. This removes the burden of maintaining an additional shared key. The extraction phase is almost same as the reverse process of embedding . Keep the count of pixels in stego image and also count of the key bits for identifying the end of data and key. After the extraction of data convert it back to ASCII string. Once the key is extracted use this same key to decrypt the data using XOR operation(In general any encryption scheme can be used for enforcing security).If the payload is of image type extract the image from the string and save it ;else if it is a text store the extracted text inside a new file.

The prototype application was implemented using python with the help of python image library (PIL) and Crypto cipher suite along with other encoding schemes like base64, binascii etc.. Using the proposed algorithm text files as well as images in png and tiff formats can be hidden , but the analysis that has been carried out in this paper mainly focuses on images. The performance analysis in terms of speed, quality and other parameters along with benchmarking of algorithm are discussed in the next section.

THE IIOAB JOURNAL
ISSN: 0976-3104

RESULTS

Analysis of Algorithm

Here the quality and performance of the algorithm based are being analyzed on the basis of various parameters like execution speed, data hiding capacity, imperceptibility, security, etc respectively. A sequential version of the algorithm was tested for determining the execution speed for various sizes and combinations of inputs namely the payload size and prime triplet combinations respectively. A graph was plotted with Input size vs. Execution time and the result is shown aside.

For a cover image size of 1024*1024 and prime triplet (13,17,19), it was observed that maximum possible size of image for hiding was 220*220 (22%);but with lower prime triplets higher resolution was possible.

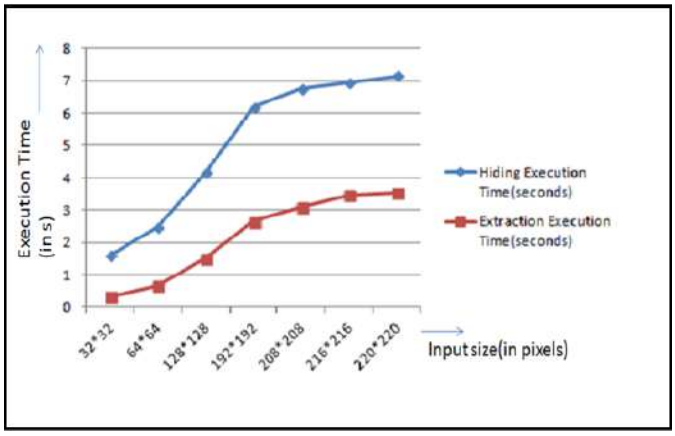

Fig: 5. Input vs. Execution Time

……..

Let m, n, p be the size of the message, key and cover image (in bits).Let (p1, p2, p3) be prime triplets. Let p>>>m, n (since cover image should be sufficiently large).Here, as observed from the flow diagram of the algorithm, for each pixel location, do '5' comparisons (p1, p2, p3, co prime-flag, end of key/message).Therefore, Total Number of comparisons = 5 * (Number of pixels used up for hiding in cover image) Number of pixels used up for hiding in cover image = At Most (m+n)/2 (worst case) (e.g. all pixel location are either exclusively multiple of any one number or a co prime) Because for each pixel store at least 2 bits of key/message in component LSB's.

i.e. $O((m+n)/2)$

So, Total no. of comparisons ,

(T.C) = $5 * O((m+n)/2)$.

If 'b' LSB bits are used then the complexity will be

T.C = $5 * O((m+n)/b)$.

Now, the Asymptotic Time Complexity for the entire algorithm is

$T(m,n) = O(m+n)$.

[Since constant terms can be neglected, assuming encryption, conversion etc. take constant time]

The parameters for measuring the performance for Steganographic algorithms are Image quality, Data Hiding Capacity, Security, Imperceptibility etc. Our main objective is to find optimum data hiding capacity with respect to all the above parameters, for this algorithm.

The data hiding capacity is generally proportional to the number of bits hidden per pixel, which is based on number of bits hidden on each component of a pixel. At maximum level hide 4 LSB bits per component of a pixel; beyond this limit, usually artifacts will become visible reducing the quality of the image. This will directly affect the imperceptibility (which is one of the major goals of Steganography) of the stego image , and thus one will be easily able to identify the discrepancy with the image. Thus an optimum value is required to maintain good data hiding capacity and at the same time have good imperceptibility. This is like a trade-off between two parameters hiding capacity and imperceptibility. In the naive implementation 4

THE IIOAB JOURNAL
ISSN: 0976-3104

LSB bits have been used for hiding the data inside cover image. The maximum modification occurs in pixels whose positional number is divisible by all the prime triplets wherein hide 4 data bits in all the three components (B, G, R) LSB position. The number of such pixels will be very low (also depends on values of prime triplets) when compared to other type of pixels. The following table shows the PSNR, MSE values for various types of inputs followed by the corresponding graphs in **Figure–1** (for PSNRs) and in **Figure–2** (for MSEs).

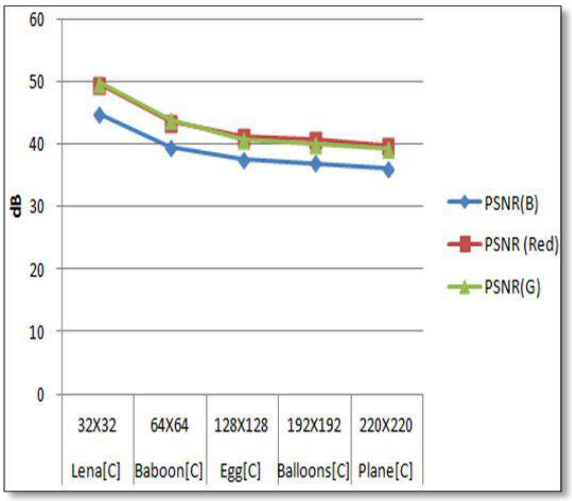

Fig: 6. PSNR - R,G,B

……..

:

Image	Size	PSNR(B)	PSNR (Red)	PSNR(G)	MSE(B)	MSE(Red)	MSE(G)
Lena[C]	32X32	44.831292	49.626305	49.876463	2.51	0.67	0.71
Baboon[C]	64X64	39.3725797	43.5099666	43.9048412	7.57	2.67	2.92
Egg[C]	128X128	37.4430374	41.2344887	40.6790346	11.81	4.93	5.61
Balloons[C]	192X192	36.8456661	40.7617169	40.0081296	13.55	5.5	6.54
Plane[C]	220X220	36.0297394	39.8449123	39.2234668	16.35	6.79	7.84

Table: 1.PSNR, MSE of R,G,B components

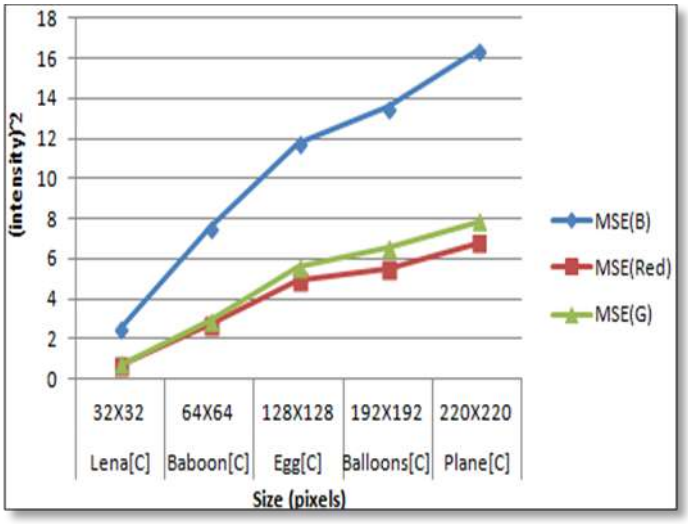

Fig: 7. MSE- R,G,B

……..

THE IIOAB JOURNAL
ISSN: 0976-3104

Different PSNR and MSE values (depicted via. the following tables):

Image	Size	PSNR(in dB)	MSE
Lena[C]	32X32	48.11	1.29
Baboon[C]	64X64	42.26	4.39
Egg[C]	128X128	39.79	7.45
Balloons[C]	192X192	39.21	8.53
Plane[C]	220X220	38.37	30.98

Table: 2. Overall PSNR,MSE (cover vs. stego)

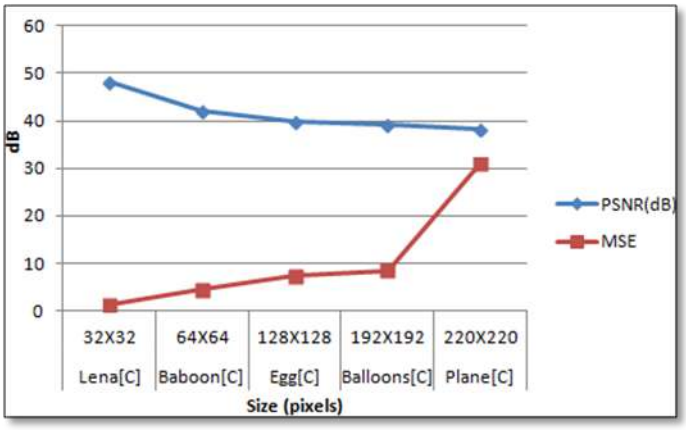

Fig: 8. Overall PSNR and MSE

Experiment and sample output

The following images were utilized for our experimentations:

Fig: 9. Images used for experimentations

As per proposed in this paper, a short implementation has been carried out and is shown below.

The image Lena.png shown above has been used as the cover image to hide payload images such as Aeroplane.jpg , Balloon.jpg,

THE IIOAB JOURNAL
ISSN: 0976-3104

Baboon.jpg, egg.jpg , etc. A sample output for hiding Baboon.jpg has been shown below.

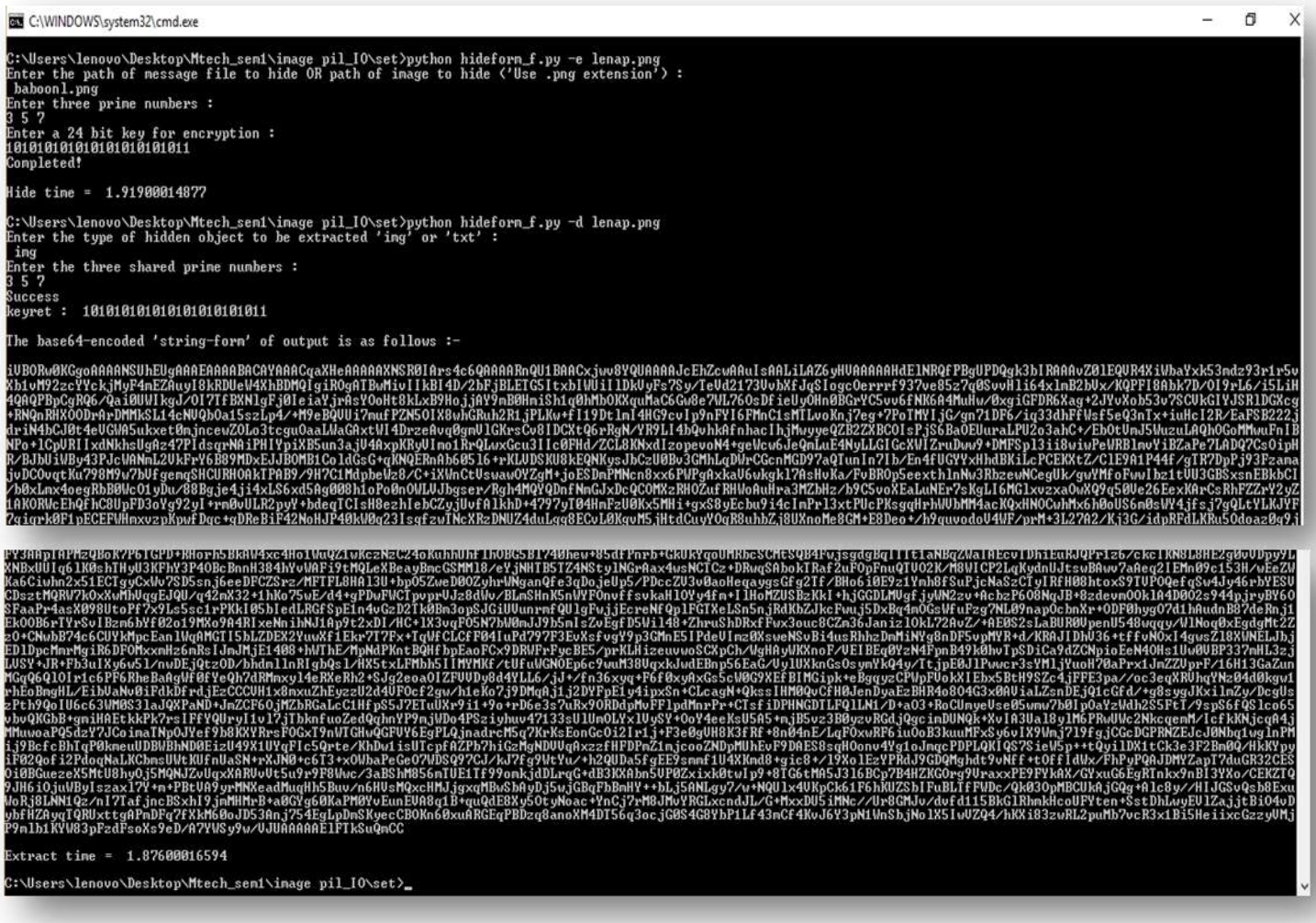

Fig: 10. Sample Outputs:

DISCUSSION

In the tables **[Tables– 1 & 2]**and graphs (depicted via. **Figures– 1, 2 & 3]** for the PSNR (Peak Signal-To-Noise Ratio) and MSE (Mean Square Error) values the following specific formulas have been used:

MSE (Mean Square Error):

It gives the mean of the pixel values of the image and by averaging the sum of squares of the error between two images.

$$MSE = \frac{\hat{}}{M * N} \rangle \quad \rangle \quad [x(m,n) - y(m,n)]^2$$

where x (m, n) and y (m, n) refers to the two images having a size of M*N. In this formula x is the original image and y is the stego image .

PSNR (Peak Signal-To-Noise Ratio):

The Peak Signal-to-Noise Ratio (PSNR) measures the estimates of the quality of the stego-image compared with an original image and is a standard (benchmark) way to measure image reliability or conformity.

ISSN: 0976-3104

$$PSNR = 20 \log_{10} \left| \frac{\text{MAXPIX}}{RMSE} \right|$$

where, MAXPIX is the maximum value of a pixel and RMSE is the Root Mean Square Error for the input image (it gives the average sum of distortion in each pixel for the stego image i.e. the average change in pixel caused by the encryption algorithm used).

In PSNR signal is the original image and noise is the error in the stego image resulting due to encoding and decoding. PSNR is measured in decibel (dB).

Also, Peak Signal to Noise Ratio (PSNR) is inversely proportional to the Mean Square Error (MSE), which implies that lower the value of Mean Square Error (MSE), higher is its Peak Signal to Noise Ratio (PSNR). Thus higher the Peak Signal to Noise Ratio (PSNR) the more is it better as it results in lesser error.

After comparing the input image(that is to be embedded in the cover image)before embedding and after extraction it was found that the MSE was zero(0.00) and PSNR value was found to be infinite(Inf dB).This confirms that the input image embedded in the cover image and the image that has been extracted are same. In the following sections comparisons of the cover and the stego images have been carried out with the help of histograms. The histograms depict the graphical representations between the intensity values of pixels (along X axis) and their frequencies (along Y axis) of the images that are being compared.

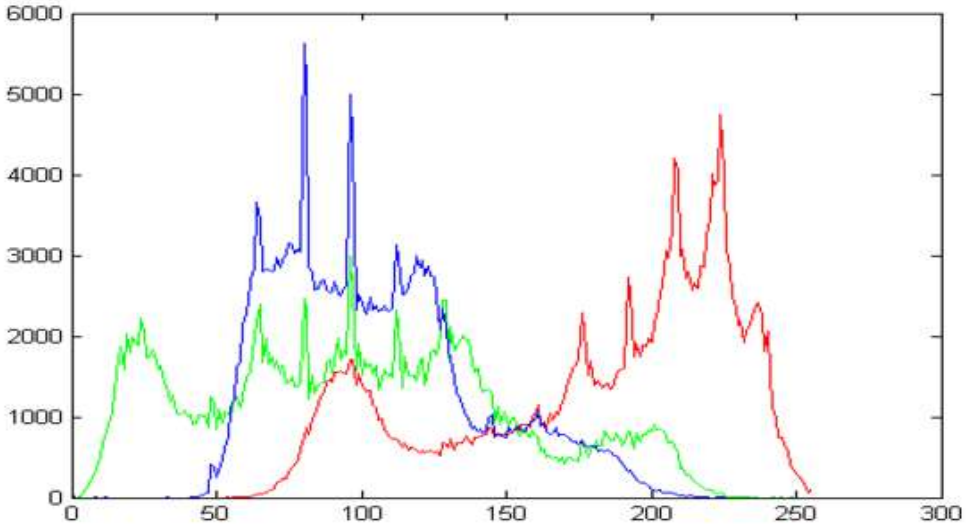

Fig: 11. Histogram before Embedding (COVER IMAGE)

Here the Cover image size was 512*512 and the payload image was 64*64.The color of the graph lines indicate the corresponding values for the R/G/B component. Histogram gives a plot of intensities of components versus. their frequencies in constituent pixels of the image. It is clear from the graph that most of the changes occur in the blue components of the pixels of the cover image followed by green and then red components are the least modified. The algorithm is a modified form of LSB substitution some extra security and also hiding capacity have been obtained. Thus it will be more difficult to crack the secret data by Steganalysis than the conventional LSB techniques. The security depends upon the encryption technique employed. Also the use of random prime triplet makes it difficult to predict the pattern of embedding. Even if the pattern is somehow decoded , still encryption provides so security against complete failure.

The prime triplet used is random and is not repeated within a particular time frame or particular number of exchanges of message using this technique. Finally the key is stored in pixel locations which are co prime to prime triplets, that too in a cyclic manner in R/G/B components for each such positions. Thus these interdependent security features, in effect provides us a high level security against the common Steganalysis techniques.

ISSN: 0976-3104

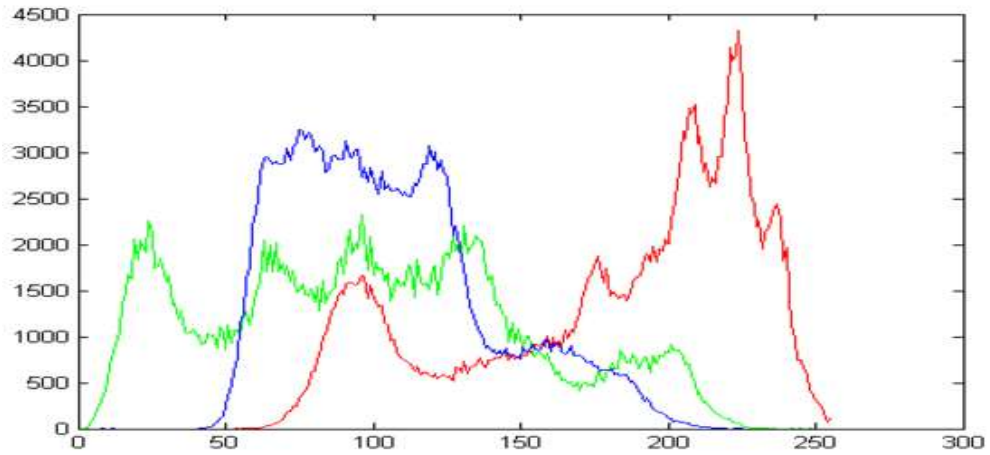

Fig: 12. Histogram after Embedding (STEGO IMAGE)

Upon comparison of some previous steganographic algorithms in [1],[11]with the proposed work, the following results have been obtained as has been described below.

COVER IMAGE	WU AND TSAI'S METHOD(PSNR in dB)	HSIEN AND HUI METHOD(PSNR in dB)	PROPOSED METHOD (PSNR in dB)
LENA	38.94	40.21	48.11
BABOON	33.43	41.35	42.26

Table: 3. Comparison of PSNR of proposed algorithm

LENA IMAGE	LSB3 METHOD	PVD METHOD	LIE CHANG'S METHOD	JAE GIL YU METHOD	FIRST COMPONENT ALTERATION TECHNIQUE	PROPOSED METHOD
PSNR	37.92	41.48	37.53	38.98	46.11	48.11

Table: 4. PSNR value comparison of lena image.

As per the comparison-based data tabulated above, the PSNR values that have been obtained by our proposed algorithm and those that of the existing ones, we infer that the proposed algorithm is superior in terms of PSNR metric. This indicates that the output images used for our experimentations have better quality and less distortions .Besides ,to make the algorithm securer ,we are using symmetric key encryption algorithms along with prime triplets which are not existing in the previous works. To verify the correctness of this proposed technique, the PSNR values of original payload image have been compared with the extracted output image. It was observed that PSNR value was infinity and the MSE value was zero. Thus successful extraction of the original image is confirmed. Likewise, the proposed technique has also been verified with text inputs. So, the proposed algorithm works well with texts and images adding flexibility and scalability to the algorithm.

CONCLUSION

In today's world, we often hear about a popular term "Hacking". This refers to an unauthorized access of data during transmission or storage. In the case of Steganography this problem is often termed as Steganalysis. This concept (basically to prevent hacking using Steganography) has been used to hide data in images, securely and efficiently. Steganography combined with Cryptography may be some of the future solutions. The general parameters for any Steganographic technique involves robustness, data-hiding capacity and security which should be optimized .A new prime-pixel alteration technique has been presented in our paper ensuring the above criteria. So future works are inclusive of extension of the

THE IIOAB JOURNAL ISSN: 0976-3104

algorithms with different image formats(like jpeg, bmp, etc) and media formats. Also this algorithm can be explored much more by using other color domains like HSI, YCBCR, etc. formats. Nowadays it is very frequent of new Steganographic techniques to be proposed and Steganalysis methods to be found. Thus emphasizing on the fact that Steganography, nowadays is an essential pre-requisite for the communications over the Internet.

FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

ACKNOWLEDGEMENT

We would like to thank the School of Computing Sciences and Engineering, VIT University and Special thanks to Dean SCOPE, for his kind guidance and support along with our guide Dr(Mrs.) Mythili Thirugnanam without whom it would not have been possible to complete this mammoth task . This work has been (Partially) supported by the research program in SCOPE, VIT University, India.

CONFLICT OF INTEREST

No conflict of interest

REFERENCES

[1] MG Gouthamanaath, A.Kangaiammal, Ph.D," Color Image Steganography using Combined Pixel Value Differenncing and Pixel Indicator Technique in Spatial Domain, *",International Journal of Computer Applications* (0975 – 8887) National Conference Research Issues in Image Analysis and Intelligence (NCRIIAMI-2015).

[2] Agham Vinit, and Tareek Pattewar.[2014] Data hiding technique by using RGB-LSB mechanism. Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE,.

[3] Darshan R Prabhu, and M Divya . [2014]Acce-leration of LSB Algorithm in GPU.(2014).

[4] Bharti, Deeksha, and Archana Kumar.Enh- anced Steganography Algorithm to Improve Security by using Vigenere Encryption and First Component Alteration

[5] Mahimah P, and R Kurinji. [2013] Zigzag pixel indicator based secret data hiding method. " Computational Intelligence and Computing Research (ICCIC), 2013 *IEEE International Conference on IEEE*,.

[6] JyothiUpadhya K.U Dinesh Acharya, and S Hemalatha.[2013] Speed-Up Improvement Using Parallel Approach in Image Steganography.

[7] Fillatre Lionel. [2012] Adaptive Steganalysis of least significant bit replacement in grayscale natural images. Signal Processing, *IEEE Transactions* on 60.2: 556–569.

[8] Hong Wien, and Tung-Shou Chen. [2012]A novel data embedding method using Forensics and Security, *IEEE Transactions* on 7(1) 176–184.

[9] Sharma Sonia, and Anjali Dua.[2012]Design and Implementation of an Steganography Algorithm Using Color Transformation. IJRTE) *International Journal of Recent Technology and Engineering* 1(2)

[10] Amirtharajan Rengarajan, et al.[2012] Who decides hiding capacity? I, the pixel intensity. Recent Advances in Computing and Software Systems (RACSS), 2012 *International Conference on. IEEE*,

[11] Kaur Amanpreet, Renu Dhir, and Geeta Sikka."A new image Steganography basedon first component alternation technique". arXiv preprint arX iv:1001.1972(2010).

[12] Luo Weiqi, Fangjun Huang, and Jiwu Huang. [2010] Edge adaptive image steganography based on LSB matching revisited. Information Forensics and Security, *IEEE Transactions o*n 5(2): 201–214.

[13] Yang, Cheng-Hsing, et al. [2008]Adaptive data hiding in edge areas of images with spatial LSB domain systems." Information Forensics and Security, IEEE Transactions on 3(3): 488–497.

[14] E Hecht.[1987] Optics, 2nd Ed, Addison Wesley,.

ABOUT AUTHORS

Mr. Anil Sathyan is currently pursuing his M.Tech Computer Science and Engineering at VIT University, Vellore ,Tamil Nadu, India. He has completed his B.Tech CSE from GEC Thrissur, Calicut University, Kerala, India. He is a an active follower of FOSS and has research interests in the field of image processing, cryptography, mobile application development and also latest web technologies. He has done various research projects in the fields of image processing, data mining and parallel computing.

THE IIOAB JOURNAL
ISSN: 0976-3104

Dr. Mythili Thirugnanam is an Associate Professor in the School of Computing Science and Engineering at VIT University, Vellore, India. She received a Master's in Software Engineering from VIT University. She has been awarded doctorate in Computer Science and Engineering at VIT University in 2014. She has teaching experience of around 8 years. She has an research experience of 3 years in handling sponsored projects funded by Govt. of India. Her area of specialization includes Image Processing, Software Engineering and Knowledge Engineering. She has published nine papers in international journals and presented around seven papers in various national and international conferences

Sumit Hazra is currently pursuing his M. Tech in Computer Science and Engineering at VIT University , Vellore which is a Research based course. He has completed his graduation (B.Tech in CSE) from Guru Nanak Institute Of Technology affiliated to West Bengal University Of Technology, Vellore in the year of 2015. He has received meritorious scholarship from VIT University for being one of the top scorers in the 1st Semester exams of his M. Tech. He has successfully completed the trainings on Advanced C,C++ and Java courses and hence been certified by IIT ,Bombay for the same, funded by National Mission on Education through ICT, MHRD, Govt., of India. Also he has been certified by the Telecom Sector Skill Council , Government Of India, for having cleared successfully the assessment for the role of Customer Care Executive(Relationship Centre) conforming to National Skill Qualifications Framework Level-4.