ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Line Based Cubism-Art Image Used for Data Hiding

Vaishali N. Ingle[1,] Dr. A.M.Patil[2]

M.E Student, Dept. of E&TC, J. T. Mahajan College of Engg., Faizpur. NMU University, Maharashtra, India[1]

Head, Dept. of E&TC, J. T. Mahajan College of Engg, Faizpur, NMU University, Maharashtra, India[2]

ABSTRACT: Data Hiding is a method that hide confidential data in a cover medium so that it can be kept as most secure. This secure data hiding method consists of two types of information, a set of secret information that is to be embedded and a set of the cover medium in which the information is kept. The main aim of data hiding is to keep the data as secure as possible and also to protect from the hackers. Data can be hided in various domains such as text, audio, video and on images. The significant importance in which the images are used for data hiding is that the human beings are very weak in analyzing the small color changes .Data can be kept secure in medical images, aerial images, texture images and also on art images. Aesthetic data hiding is a new form of data hiding by the use of art image generated by some art image generation algorithm. People are attracted by the art image and thus they are not noticed about the hidden data. Thus data can be kept more securely. Cubism images are a type of paintings in which they are formed by analyzing an image or objects from multiple viewpoints. Cubism paintings are composed of intersecting line segments and various regions from different viewpoints. Line-Based Cubism Art image is created based on the concepts of cubism art. Data Hiding and lossless recovery is carried out with security measures secre. in this paper we have proposed a new technique of image stegnography i.e Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form.

KEYWORDS: Computer art image,line-based cubism-like image,steganography,Hash-LSB,RSA Encryption-Decryption

I. INTRODUCTION

Data hiding is a promising and secure technique for information security, authentication, copyright protection, etc. Data hiding means information represented by some data are hidden in a cover medium to kept these data as secure. Different data hiding algorithms are implemented on images. But in most cases, the cover media is permanently distorted due to data hiding and thus the original medium is difficult to restore. Due to this there is no proper way to recover the marked media back to the original media without distortion. In least significant bit-plane (LSB) embedding method, the LSB bits are replaced with the data and the bit replacement is difficult to memorize and thus this method is not invertible.

A new method of data hiding by using art image generation algorithm enhances the camouflage effect for various information-hiding application is proposed.an art image created by source image based on cubism properties is called line-based cubism art image. Cubism artists transform a natural scene into geometric forms in paintings by breaking up, analyzing and reassembling objects in the scene from multiple viewpoints. In addition, with the scene objects rearranged to intersect at random angles, each Cubism painting seems to be composed of intersecting lines and fragmented regions in an abstract style. The idea of the proposed art image creation technique is inspired by these concepts of the Cubism art. Specifically, there are two major stages in the proposed linebased Cubism-like image generation process—prominent line extraction and region recoloring. In the first stage, at first we extract line segments from a given source image by edge detection and the Hough transform. Then, we conduct short line segment filtering and nearby line merging. In the second stage, at first we create regions in the image by extending the line segments to the image boundary to partition the image space. Then, we recolor the regions by the average region colors and whiten the boundaries of the regions.

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in cryptography it's always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. Data hiding process is illustrated in Fig. 1.

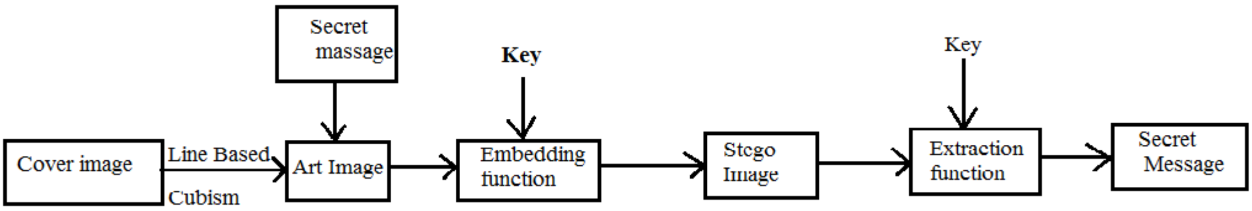


Fig.1Block diagram of process

A. Cryptography

The field of cryptography has a rich and important history, ranging from pen and paper methods, to specially built machines, to the mathematical functions that are used today. In this paper only brief discussion that is essential for knowledge transfer has been presented. Cryptology is the science of coding and decoding secret messages. (Cryptology is the Greek root for secret or hidden). It is usually divided into cryptography, which concerns designing cryptosystems for coding and decoding messages. It states that the term cryptography generally refers to the collection of cryptographic mechanisms that include:

- Encryption and decryption algorithms
- Integrity check functions
- Digital signature schemes

B. Steganography

Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. Generally this can be done by embedding the secret message within another digital medium such as text, image, audio or video. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphie meaning "writing" . The first recorded use of the term was in 1499 by Johannes Trithemius in his Stegano-graphia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other "cover-text" and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is a high security technique for long data transmission. There are various methods of steganography:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion techniques

II. Related work

There are many steganography techniques which are capable of hiding data within an image. These techniques can be classified into two categories based on their algorithms: (1) spatial domain based techniques; (2) transform domain based techniques [14]. The spatial domain based steganography technique use either the LSB or Bit Plane Complexity Segmentation (BPCS) algorithm [22]. The most widely used technique to hide data is the usage of the LSB [6]. The existing techniques are mainly based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits. A significant number of methods have been proposed for LSB steganography [1], [2], [3], [4], [9], [11], [13], [17], [18], [19], [23].C. K. Chan and L. M. Cheng proposed datahiding using simple LSB [29] substitution method. This is one of the earliest data hiding techniques. Here data embedding to encrypted key is done by changing the LSB of the encrypted image using data hiding key. Least significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity. The fundamental idea here is to insert the secret message in the least significant bits of the images. This actually works because the human visual system is not sensitive enough to pick out changes in colour. A basic algorithm for LSB substitution is to take the first N cover a pixel where N is the first letter of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits. The LSB or in other words 8-th bit of some or all the bytes inside an image is changed to a bit of the secret message.J. Tian et al. [31] proposed a method of reversible data hiding using difference expansion. Reversible data hiding can provide the extracted data and the original image without degradation at receiver side. This is most useful in areas where we strictly require keeping the quality of the image even though we are embedding data in it. This is used areas like water marking, cover authentication etc. Masud et al. [1] has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. In [3], [4], [21], [23] and [25] designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used. In [9] proposed a LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. Mohmmad A.Ahmed et al. [17] proposed a method in which a message hidden inside an image by using the Least Significant Bit technique and after creation of the hidden message, the image will pass it in hash function to obtain hashing value using the MD5 technique. In [18] two steganography technique proposed for hiding image in an image using LSB method for 24 bit color images. In [19] a hash based approach proposed for secure keyless steganography in lossless RGB images that an improved steganography approach for hiding text messages in lossless RGB images. The paper [5], [8], [16], and [20] provides an overview of image steganography, its uses and analysis of various steganography techniques. In [15] a security analysis on spatial domain steganography for JPEG decompressed images has been presented. Anderson and Petitcolas [10] posed many of the open problems resolved in this article regarding to steganography. In particular, they pointed out that it was unclear how to prove the security of a steganographic protocol. They also posed the open question of bounding the bandwidth that can be securely achieved over a given cover channel. Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exist to implement video steganography [2], [7]. In [2] a hash based least significant bit technique for video steganography has been proposed. Where the secret information is embedded in the LSB of the cover frames and a hash function is used to select the position of insertion in LSB bits. In paper [7] proposes a secure covert communication model based on video steganography which is based on pixel-wise manipulation of colored raw video files to embed the secret data.

III. Existing Techniques Used

I. Proposed Line-Based Cubism-Like Image Creation Process

Cubism artists transform a natural scene into geometric forms in paintings by breaking up, analyzing and reassembling objects in the scene from multiple viewpoints. In addition, with the scene objects rearranged to intersect at random angles, each Cubism painting seems to be composed of intersecting lines and fragmented regions in an abstract style. The idea of the proposed art image creation technique is inspired by these concepts of the Cubism art. Specifically, there are two major stages in the proposed linebased Cubism-like image generation process—prominent line extraction and region recoloring. In the first stage, at first we extract line segments from a given source image by edge detection and the Hough transform. Then, we conduct short line segment filtering and nearby line merging. In the second stage, at first we create regions in the image by extending the line segments to the image boundary to partition the image space. Then, we recolor the regions by the average region colors and whiten the boundaries of the regions.

There are a large number of cryptographic and steganographic methods that most of us are familiar with. The most widely used two techniques are:

- RSA Algorithm
- LSB Insertion Method

A. RSA Algorithm

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure. RSA algorithm procedure can be illustrated in brief as follows : (i) Select two large strong prime numbers, p and q. Let n = p q. (ii) Compute Euler's totient value for n: f (n) = (p - 1) (q - 1).

(iii)Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.

(iv)Calculate a number d such that d = e-1 mod f (n). (v) Encryption: Given a plain text m satisfying m < n, then the Cipher text c= m^e mod n. (vi) Decryption: The cipher text is decrypted by m = c^d mod n.

B. Least Significant Bit (LSB) Insertion Method

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image [16]. For an 8-bit image, the least significant bit i.e. the 8_{th} bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number [16]. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images).

IV. Problem Formulation and Work Methodology

The problem statement consists of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding the secret message have to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called Hash-LSB derived from LSB insertion on images. In this Hash-LSB, we are using a hash function to evaluate the positions where to hide the data bits or to be embedded. It is a challenging process which will lead us to combine the two technologies, one of them is RSA algorithm from cryptography and other is Hash-LSB from steganography. Our research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or intruders. We have used Hash-LSB and RSA algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data.

A. Cover Image and Secret Message

In our proposed system, first of all we select a true colour image of size 512 x 512 for to it as a cover image then create cubism art image Specifically, there are two major stages in the proposed line based Cubism-like image generation process— 1)prominent line extraction (2) region recoloring.

In the first stage, at first we extract line segments from a given source image by edge detection and the Hough transform. Then, we ignore the short line segment and nearby line merging. In the second stage, at first we create regions in the image by extending the line segments to the image boundary to partition the image space. Then, we recolor the regions by the average region colors and whiten the boundaries of the regions and a secret message which will be embedded in the Art image.

Cubism Art image creation Algorithm:-

Stage 1-Prominent line extraction.

Step 1.perform Canny edge detection to find the edge points in source image S,thus producing in a new image s'.
Step 2.perform the following steps to find prominent line segments in S'
2.1.find line segments $L_{1,}L_{2,\ldots\ldots,}L_{m\,,}$in S' by applying the Hough transform on S' ,results in a second new image S".
2.2.Select the prominent line segments in S" with lengths larger than threshold value $L_{min.}$
2.3 Compare every line pair Li and Lj with i $\neq$ j in S" and if the distance Dij between Li and Lj is smaller than

D_{min}, then delete Li if the length of Li is smaller than that of Lj ;or delete Lj , otherwise.
Step 3. Extend each of the remaining line segments in S" to the boundaries of S", and regard the source image S as being partitioned by these extended lines to form regions.

Stage 2 Re-coloring regions.

Step 4. (*Line extension*) Extend each remaining line segment in *S"* to the image boundaries of *S* ".
Step 5. (*Region Partitioning*) Partition *S*"in to regions *R1,R2,…,Rk* by the extended lines.
Step 6. (*Region recoloring*) Recolor each region *Ri* in *S*" by the following steps with *i=1,2,…,k*.
6.1 Compute the area *Ai* (in unit of pixel) of *Ri* and the average color (*Cir,Cig,Cib*)of all the pixels in *Ri*.
6.2 Recolor each pixel in *Ri* by (*Cir,Cig,Cib*) .
Step7.(*Line recoloring*) Recolor all region boundaries in *S*" by the white color.
Step 8. Take the final *S*" as the desired line-based Cubism like image *Sc*.

B. Hash-LSB (Least Significant Bit) Process

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function. Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will uses the values given by hash function to embed or conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively. According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB as illustrated in Fig. 2. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image .

$$k = p \,\%\, n \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (1)$$

where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining of bits into information will produce the secret message as required by the receiver.

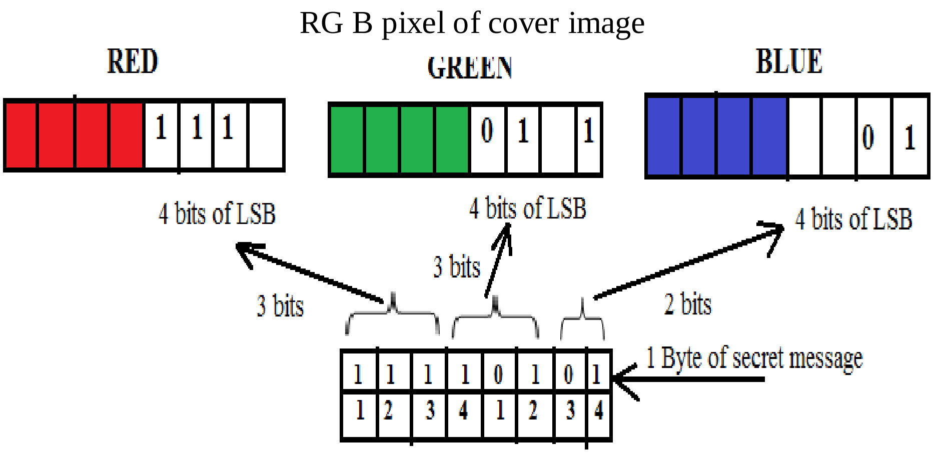


Fig.2.(a)

Consider a RGB Pixel of cover image

MSB RED LSB

0	0	1	0	0	1	1	1

MSB GREEN LSB

1	1	1	0	1	0	0	1

MSB BLUE LSB

1	1	0	0	1	0	0	0

Also suppose 245 is that value of the secret data byte after converted converted it into binary value is 11110101. It is distributed in the order of 3, 3, and 2 to be embedded in LSB of RGB pixels respectively.

Let the hash function of equation (1) returns values of k=1, 2, 3 for R, k=4, 1, 2 for G and k=3, 4 for B.

So the after embedding the secret data in the particular positions of RGB value of cover image the RGB pixel value of stego image is given below.

MSB R LSB

0	0	1	0	1	1	1	1

MSB G LSB

1	1	1	0	0	1	0	1

MSB B LSB

1	1	0	0	1	0	0	1

Fig.2.(b)

Fig.2.(a)-(b) Hash process to find LSB of RGB pixels value

C. RSA Encryption and Hash-LSB Encoding

This approach of image steganography is using RSA encryption technique to encrypt the secret data. Encryption includes a message or a file encryption for converting it into the cipher text. Encryption process will use recipient public key to encrypt secret data. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key. At the start of this process we take cipher text encrypted from the secret message to be embedded in the cover image. In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image .

Embedding Algorithm:
Step 1: select cover image.
Step2: Read secret message.

Step 3: Encrypt the message using RSA algorithm.
Step 4: Find 4 least significant bits of each RGB pixels from cover image.
Step 5: Apply a hash function on LSB of cover image to get the position.
Step 6: Embed 8-bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3,3&2 respectively using the position obtained from hash function given in equation 1.
Step 7: send stego image to receiver.
Step 8: repeat step 4 to 7 until all pixels of stego images are embedded in cover image.

D. Hash-LSB Decoding and RSA Decryption

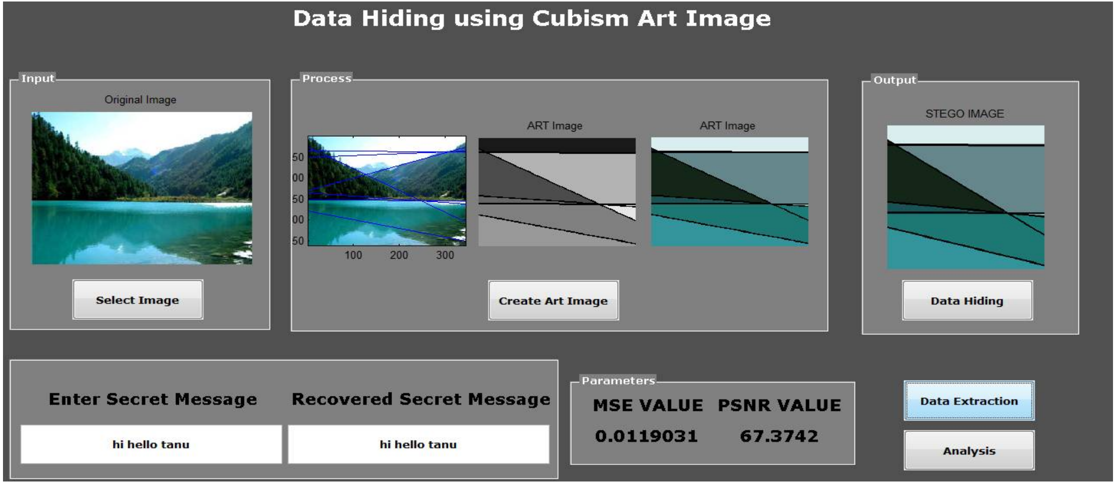
In the decoding process we have again used the hash function to detect the positions of the LSB's where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form.

Retrieval Algorithm:
Step 1: Receive a stego image.
Step 2: Find 4 LSB bits of each RGB pixels of the stego image.
Step 3: Apply hash function to get the position of LSB's with hidden data.
Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
Step 5: Apply RSA algorithm to decrypt the retrieved data.
Step 6: Finally read the secret message.
Step 7: Repeat steps 3 to 6 until all pixels of secret image embedded are retrieved.

V. PERFORMANCE ANALYSIS AND RESULTS

In this paper the line based cubism art image is created based on the features of the cubism art. The implementation is done with an input source image, relevant line segments in the image are detected and rearranged to form an art image of the Cubism flavor. Data hiding is done by using Hash LSB method with RSA algorithm.

Fig.3 shows the results of applying the Hash LSB method with RSA algorithm for data hiding to cubism-like image. first generated Cubism –like images using algorithm 1& 2 with no message data embedded. Then stego image into which a message data string "Hi hello tanu." it has been embedded .As can be seen, the stego-image is almost identical to cover art image. In addition, the stego-image qualities are good after the average region colors are changed for data embedding,as indicated by the very small MSE and high PSNR values listed in below.



Enter Secret Message: hi hello tanu
Recovered Secret Message: hi hello tanu

MSE VALUE 0.0119031 PSNR VALUE 67.3742

Fig.3.PSNR & MSE Values of stego image with respect to generated Art Image.

VI. COMPARISONS WITH OTHER LSB DATA HIDING METHOD.

The objective of the work have been implemented an image steganography technique using Hash-LSB (Least Significant Bit) method with RSA algorithm to improve the security of the data hiding technique. This technique is a combination of one steganographic technique and one cryptographic technique which enhances the security of data and data hiding technique. Our implemented Hash-LSB technique on images is used to hide information in the RGB pixels value of the cover image in the form of 3, 3, and 2 bit order and positions to hide the data bits have been calculated by hash function. The use of RSA algorithm has made our technique more secure for open channel. RSA algorithm has been used with Hash-LSB so that the original text will be embedded into cover image in the form of cipher text. The Hash-LSB technique has been applied to true color images and which gives satisfactory results. The performance of the Hash-LSB technique has been evaluated and graphically represented on the basis of two measures are – Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) and obtained values are much better than existing techniques. The technique called "A Secure Steganography Based on RSA Algorithm and Hash-LSB Technique" has been implemented on MATLAB tool by analyzing four color images of size 512 x 512 tiff format as selected to hide a fixed size of secret data. In this process stego-image is generated using Hash-LSB and RSA encryption which carried out to enhance the security of hidden data.

For the performance analysis of the Hash-LSB technique to be implemented on four covers images Barbara, Tulips,Lena, and Baboon are considered and shown in the Fig. 4

(a) Barbara(b) Tulips (c) Lena (d) Baboon

Fig.4.(a)-(d) four cover images

The results for all stego images using Hash-LSB with RSA technique have been compared to simple LSB substitution (Reversible LSB &Irreversible LSB) with RSA technique which gives very lesser MSE values and higher PSNR values. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) between the stego Image and its corresponding cover image have been studied and given below as eq. 2 and 3.

$$MSE=\frac{1}{H*W}\sum_{i=1}^{H}(P(i,j)-S(i,j))^{2}\text{………….... (2)}$$

Where, MSE is Mean Square Error, H and W are height, width and P (i, j) which represents the cover image and S (i, j) represents its corresponding stego image.

$$PSNR=10log\ 10\frac{L^{2}}{MSE}\text{…………. (3)}$$

Where, PSNR is peak signal to noise ratio, L is peak signal level for a color image have been taken as 255. In this technique of image steganography eight bits of data are embedded in 3 pixels of the cover image. The mean square error (MSE) and the peak signal to noise ratio (PSNR) for different stego images are shown in the Table I. By comparing the PSNR values of all the stego images, it has been analyzed that only Lena as a cover image have given the best PSNR value. The same is true in the case for the MSE values while comparing with different stego images, Lenna as a cover image have given the least MSE value.

Table I. Results obtained from Irreversible LSB,Reversible LSB & H-LSB with RSA technique

Name of the image file	Result obtained using Irreversible LSB with RSA		Result obtained using Reversible LSB with RSA		Result obtained using Hash LSB with RSA	
	PSNR (db)	MSE	PSNR (db)	MSE	PSNR(db)	MSE
Baboon	34.0121	2.7655	40.0111	2.9888	44.0111	2.5666
Barbara	34.9872	2.4888	40.9888	2.5111	45.9888	2.2667
Lena	32.5899	3.4878	38.5899	3.5666	43.5666	3.2455
Tulips	32.0458	4.3444	38.0111	4.4565	42.0145	4.0000

1) Fig .5. Shows the cover image & stego image of Barbara. The PSNR (db) & MSE values have been shown.

Image 1 :-cover image Image 2:- stego image

Fig.5 PSNR & MSE values between original cover image & stego image of Barbara.

PSNR between Image (1) & Image (2) = 73.5444

MSE between Image (1) & (2) = 0.0029

2) Fig.6.shows the cover image & stego image of Lena. The PSNR & MSE values have been shown between Original image & stego image of Lena.

Image 3:- cover image Image 4:- stego image

Fig.6.PSNR & MSE values between original cover image & stego image of Lena

PSNR between Image (3) & Image (4) =74.0189

MSE between Image (3) & Image (4) = 0.0026

3) Fig. 7 shows the cover image of Tulips & stego image of Tulips. The PSNR & MSE values have been shown between original Tulips cover image & tulips stego image.

Image 5:-cover image image 6:- stego image

Fig.7.PSNR & MSE values between original cover image & stego image of Tulips

PSNR between Image (5) & image (6) =73.8220

MSE between Image (5) & image (6) = 0.0027

4) Fig. 8 shows the cover image of Baboon & stego image of Baboon. The PSNR & MSE values have been shown between original Baboon cover image & Baboon stego image.

Image 7:-cover image   image 8:- stego image

Fig.8.PSNR & MSE values between original cover image & stego image of Baboon

PSNR between Image (7) & image (8) =73.8528

MSE between Image (7) & image (8) = 0.0027

In Fig. 9, the graphical representation of PSNR & MSE values of different stego images. The horizontal axis shows the stego images and vertical shows the range of PSNR value in decibel & MSE value. The Fig.9 (a).shows the red line shows HLSB with RSA technique, green line shows the Irreversible LSB technique. & Blue line shows the Reversible-LSB.The MSE values for other LSB technique are higher than the MSE values of H-LSB with RSA as compared in both figures.

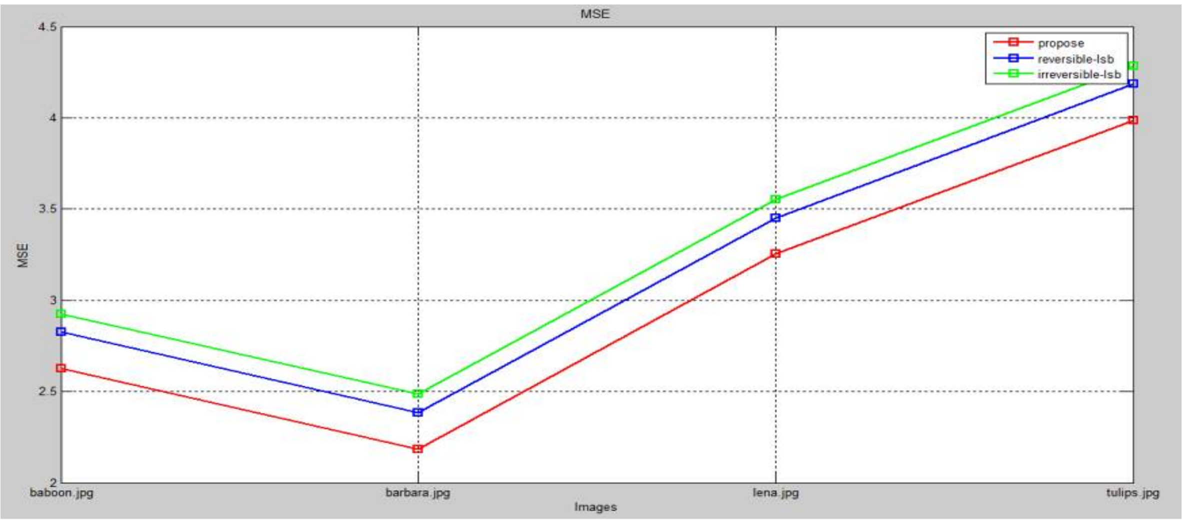


Fig. 9(a).The graphical representation of MSE value

The Fig.9 (b).shows the graphical representation of PSNR value fig. shows the red line shows HLSB with RSA technique, green line shows the Irreversible LSB technique. & Blue line shows the Reversible-LSB.The PSNR values for other LSB techniques are lesser than the MSE values of H-LSB with RSA as compared in both figures.

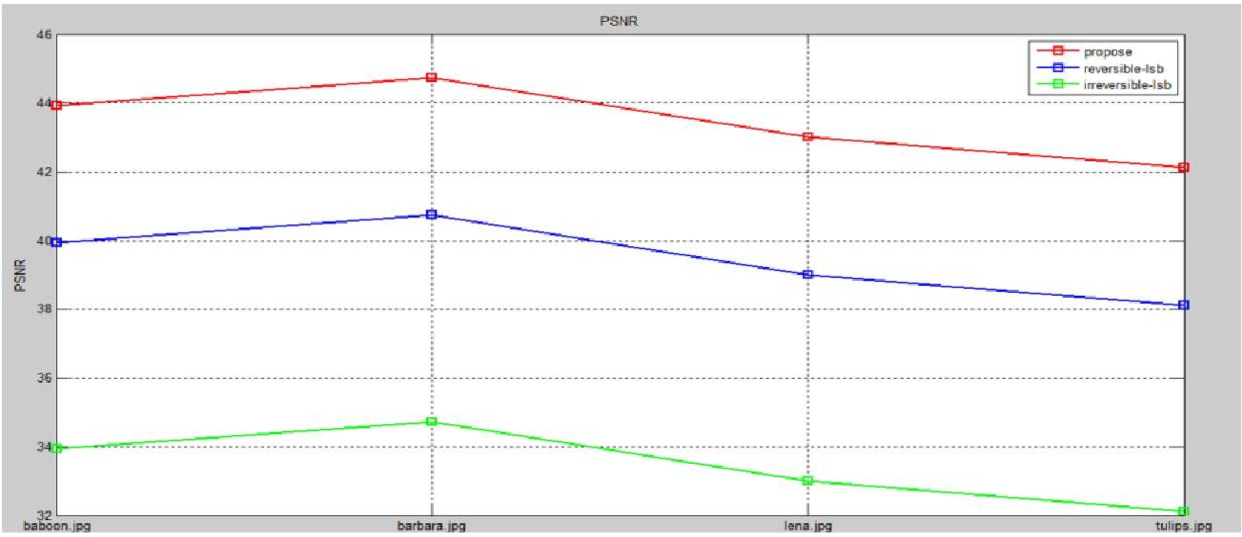


Fig.9(b).The graphical representation of PSNR value

VII. CONCLUSION & FUTURE SCOPE

In this work a new data hiding method is introduced the combining Hash-LSB with RSA algorithm method with cubism art image .A secured Hash based LSB technique for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient. This technique also applies a cryptographic method i.e.RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that’s why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The H-LSB technique have been applied to .tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

REFERENCES

1. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain “*A New Approach for LSB Based Image Steganography using Secret Key*”, International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.
2. Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, “*Hash Based Least Significant Bit Technique for Video Steganography (HLSB)*”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.
3. Mamta Juneja, Parvinder Singh Sandhu, “*Designing of Robust Image Steganography Technique Based on LSBInsertion and Encryption*”, International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.
4. Swati Tiwari, R. P. Mahajan, “*A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion*”, International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.
5. N. F. Johnson, S. Jajodia, "*Steganography: seeing the unseen*”, IEEE Computer, Vol. 31, Issue No. 2, Pages No 26 - 34, Feb., 1998.
6. Wien Hong, Tung-Shou Chen, “*A Novel Data Embedding Method Using Adaptive Pixel Pair Matching*”,IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.
7. Amr A. Hanafy, Gouda I. Salama, Yahya Z. Mohasseb, “*A Secure Covert Communication Model Based on Video Steganography*”, Military Communications Conference, IEEE, Pages No. 1 – 6, 16-19 Nov., 2008.

8. R. Chandramouli, N. Memon, "*Analysis of LSB based image Steganography techniques*", International Conference on Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.
9. Weiqi Luo, Fangjun Huang, Jiwu Huang, "*Edge Adaptive Image Steganography Based on LSB Matching Revisited*", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214, June, 2010.
10. Ross J. Anderson, Fabien A. P. Petitcolas, "*On the Limits of Steganography*", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.
11. Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "*A High Capacity 3D Steganography Algorithm*", IEEE Transactions on Visualization and Computer Graphics,Vol. 15, Issue No. 2, Pages No. 274– 284, March-April, 2009.
12. Nicholas Hopper, Luis von Ahn, John Langford, "*Provably Secure Steganography*", IEEE Transactions on Computers, Vol. 58, Issue No. 5, Pages No. 662 – 676, May, 2009.
13. Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "*RGB Intensity Based Variable-Bits Image Steganography*", Asia-Pacific Services Computing Conference, IEEE, Pages No. 1322 – 1327, 9-12 Dec., 2008.
14. Jing-Ming Guo, Thanh-Nam Le, "*Secret Communication Using JPEG Double Compression*", Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879 – 882, Oct., 2010.
15. Weiqi Luo, Yuangen Wang, Jiwu Huang, "*Security Analysis on Spatial 1 Steganography for JPEG Decompressed Images*", Signal Processing Letters, IEEE, Vol. 18, Issue No. 1, Pages No. 39 – 42, Jan., 2011.
16. Dr.Ekta Walia, Payal Jainb, Navdeep, "*An Analysis of LSB & DCT based Steganography*", Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.
17. Mohammad A. Ahmad, Dr. Imad Alshaikhli, Sondos O. Alhussainan, "*Achieving Security for Images by LSB and MD5*", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No.127-139, Sept., 2012.
18. Deepesh Rawat, Vijaya Bhandari, "*A Steganography Technique for Hiding Image in an Image using Method for 24 Bit Color Image*", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.
19. Ankit Chaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "*A Hash based Approach for SecureKeyless Steganography in Lossless RGB Images*", 22nd International Conference on Computer Graphics and Vision, 2012.
20. R. Amirtharajan, R. Akila, P. Deepika chowdavarapu, "*A Comparative Analysis of Image Steganography*" International Journal of Computer Applications, Vol. 2, Issue No. 3, May, 2010.
21. Samir Kumar Bandyopadhyay, Sarthak Parui, "*A Method for Public Key Method of Steganography*", International Journal of Computer Applications, Vol. 6, Issue No. 3, Sept., 2010.
22. P. Nithyanandam, T. Ravichandran, N. M.Santron, E. Priyadarshini, "*A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding*", International Journal of Computer Science and Security (IJCSS), Vol. 5, Issue No. 5, 2011.
23. Shailender Gupta, Ankur Goyal, Bharat Bhushan, "*Information Hiding Using Least Significant Bit Steganography and Cryptography*", I. J. Modern Education and Computer Science, Vol. 6, Pages No. 27-34, 2012.
24. Mritha Ramalingam, "Stego Machine –Video Steganography using Modified LSB Algorithm", World Academy of Science, Engineering and Technology, Pages No. 50, 2011.
25. Deepali, "*Steganography with Data Integrity*", International Journal of Computational Engineering Research, Vol. 2, Issue No. 7, 2012.
26. Asad.M., Gilani, J., Khalid.A., "*An enhanced least significant bit modification technique for audio steganography*", Computer Networks and Information Technology (ICCNIT), IEEE, Pages No. 143 – 147,11-13 July, 2011.
27. Information about cryptography, available at http://en.wikipedia.org/wiki/Cryptography.
28. Chandra.M.Kota, Cherif Aissi, "*Implementation of the RSA algorithm and its cryptanalysis*", ASEE GulfSouthwest Annual Conference, American Society for Engineering Education, USA, 2002.
29. C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition Society., vol. 37, pp. 469–474, Mar. 2003.
30. J. K. Mandal and A. Khamrui "A Data Embedding Technique for Gray scale Image Using Genetic Algorithm",ICES-2011
31. J. Tian, "Reversible data embedding using a difference expansion, "IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug.2003.
32. J. Canny, "A computational approach to edge detection," IEEE Trans.Pattern Anal. Mach.Intell., vol. 8, no. 6pp. 679–698, Nov. 1986.
33. Wen Chung Kuo and Dong- Jin-Jiang "Reversible data hiding based on histogram", ICIC-2007 Springer Verlag Berlin Heideberg.
34. vinsa Varghese,ragesh G.K "A secure method for hiding secret data on cubism Image using Hybrid featuredetection method."International Journal of Research in Engineering and Technology,vol.03,page no.43-47,Dec-2014.
35. Marghny Mohamed1, Fadwa Al-Afari2 and Mohamed Bamatraf "Data Hiding by LSB Substitution Using
Genetic Optimal Key-Permutation", International Arab Journal of e-Technology, Vol. 2, January 2011.
36. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav "Steganography Using Least Signicant Bit Algorithm" International Journal of Engineering Research and Applications Vol. 2, pp. 338-341 , May-Jun 2012
37. Shan-Chun Liu and Wen-Hsiang "Line-Based Cubism-Like Image—A New Type of Art Image and its Application to Lossless Data Hiding" IEEE ,October 2012.
38. Richu Shibu,ER.Gripsy paul "survey on data hiding technique."International Journal of Research in computer and communication technology,vol.2, page no.85-87,Nov 2011
39. Kousik Dasgupta, J.K.Mandal,Paramartha Dutta, "Hash based least significant bit technique for videostegnography (HLSB)."Vol.1,no.2,April 2012.