ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Loseless and Reversible Data Hiding Using AES and LSB

D. Diviya Bharathy

M. E Student, Department of CSE, Indraganesan College of Engineering, Trichy, Tamilnadu, India

ABSTRACT: The rapidly proliferated information and evolution of digital technologies by Information hiding in multimedia data has improved the ease of access to digital information enabling reliable, faster and efficient storage, transfer and processing of digital data and leads to the consequence of making the illegal production and redistribution of digital media easy and undetectable. Reversible data hiding is a technique by using which we can embed essential data into images, audio, video and so on. This system applies a method of hiding data in an image and videobefore encryption. The proposed scheme increases the amount of data that can be hidden in the image or video which also guarantees the lossless recovery of image or video after extraction is completed.Steganography, is a better technique for writing the hidden messages in another file format like text, image, and videos. we proposed a technique of data hiding using interpolation, least significant bit, digital watermarking and cryptography. Performance is tested through the measures mean squared error (MSE) & peak signal to noise ratio and data embedding capacity. Result shows with these parameter are shows better results from the previous results. Secret information is got from the user. The information is encrypted based on AES encryption algorithm. The encrypted information is hided in the image based on the LSB embedding algorithm. The main objective of the process is to embed the secret information in the images and to extract the secret information from the images without producing much distractions in the images. To encrypt the secret information's using AES encryption. To embed the encrypted information's using LSB embedding process. To preserve the originality in the secret information while retrieving.To measure the overall performance of the process in terms of PSNR, MSE and embedding ratio.

KEYWORDS: loseless data hiding, reversible data hiding, image encryption and decryption.

I.INTRODUCTION

Steganography is the art of hiding a file, image, or secret message within another message, image, or file. Steganography technique is that which is basically used for information security. Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. Steganography is not to alter the structure of the secret message, but hides it inside a cover object. After hiding process cover object &stego object are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Detecting procedure of steganography known as Steganalysis. Some of the applications of Steganography include ownership protection, proof for authentication, air traffic monitoring, medical applications etc. Steganography is the practice of hiding secret messages within cover image to produce a stego image. The recipient of a stego image can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego image.

Information hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academic. It contains two main branches: digital watermarking and steganography with cryptography. The carrier for steganography can be image, text, audio and video. Multimedia data is easy to destroy by the unauthorized persons through Internet. So, it becomes important to be able to transmit the data secretly. In steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen.A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganography methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Steganography software is becoming effective in hiding information in image, video, audio or text files. Most used steganography technique in least significant bit. The main objective of Steganography is to communicate securely in such a way that the true message is not visible to the observer. That is unwanted parties should not be able to distinguish any sense between cover-image (image not containing any secret message) and stego image (modified cover-image that containing secret message). Thus the stego image should not deviate much from original cover image. Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it.
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 is done by embedding the secret message within another digital medium such as text, image, audio or video. Nowadays, information is rapidly available through the Internet.

II.PROBLEM DESCRIPTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications.

Data hiding is a method used in object-oriented programming to hide information within computer code. Objects within a code are not privy to information considered hidden. It presents several advantages for programmers, because objects are unable to connect to irrelevant data and hackers are less likely to be able to access data. At the same time, hiding data can make it harder for a programmer, who may need to use more code to create effects in hidden data than would be necessary if the data were public.

The encryption process is more secure and the information's were well preserved in the image. The embedding ratio is improved.The process is reversible. The distortions will be much reduced in the stego image. Data Security is widely used to ensure security in communication, data storage and transmission. The advantage of LSB-based method is easy to implement and high message pay-load. The proposed method is a lossless encryption technique and hence can be widely employed in all the cases. The performance of the process is also much improved.

III.METHODOLOGY

The overall process in the proposed approach is the identification of the secret information hided in the input image. The secret information is got from the user. The secret information may be in the form of text data. The secret information's were encrypted with the help of AES encryption algorithm. The encrypted information is then embedded in the video frame with the help of the LSB (Bit-Plane Complexity Segmentation Steganography) algorithm. The image into which the data has be hided were divided into 8 x 8 blocks. The complexity of the block is identified.

If the complexity of the block is greater than 0.3 then the particular plane is used for embedding. Using LSB embedding data is embedding in the identified block. The stego image obtained in this process is forwarded to the receiver.

The same process is reversed in the receiver side in order to get the secret information that is hided in the image. The performance of the process is measured with the help of the performance metrics like PSNR, MSE and Embedding ratio. The proposed method performances were much improved compared to the existing methods. In the proposed system, the LSB algorithm is used to hide the encrypted data into the Encrypted image.At the time of steganography separate each pixel RGB bit and then create the 8*8 matrix and calculate the alpha value knows as Complexity. Calculating the alpha value shows that given matrix is capable of hiding some bit or not. The standard alpha value is 0.3 taken here. For calculating alpha

alpha = (Horizontal transitivity *vertical transitivity)/max transition.

Encryption and data hiding are two effective means of data protection. The additional data are embedded into a data space that is invariable to encryption operations. In another type of the works , data embedding is performed in encrypted domain, and an authorized receiver can recover the original plaintext cover image and extract the embedded data. This techniques is termed as reversible data hiding in encrypted images. In the fig 3.1 describes the original

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

image is encrypted by an exclusive or operation with pseudo-random bits, and then the additional data are embedded by flipping a part of least significant bits (LSB) of encrypted image. In each additional bit is embedded into a block of data encrypted by advanced encryption standard.

Data extraction before image decryption Consider the scenario that a low level server ,who is not granted the authority to get access to original images in consideration of protecting clients' privacy, may have the duty to note and modify the personal information in corresponding encrypted images as well as to verify images' integrity. A possible solution to this case must guarantee the independence between data extraction and image decryption.

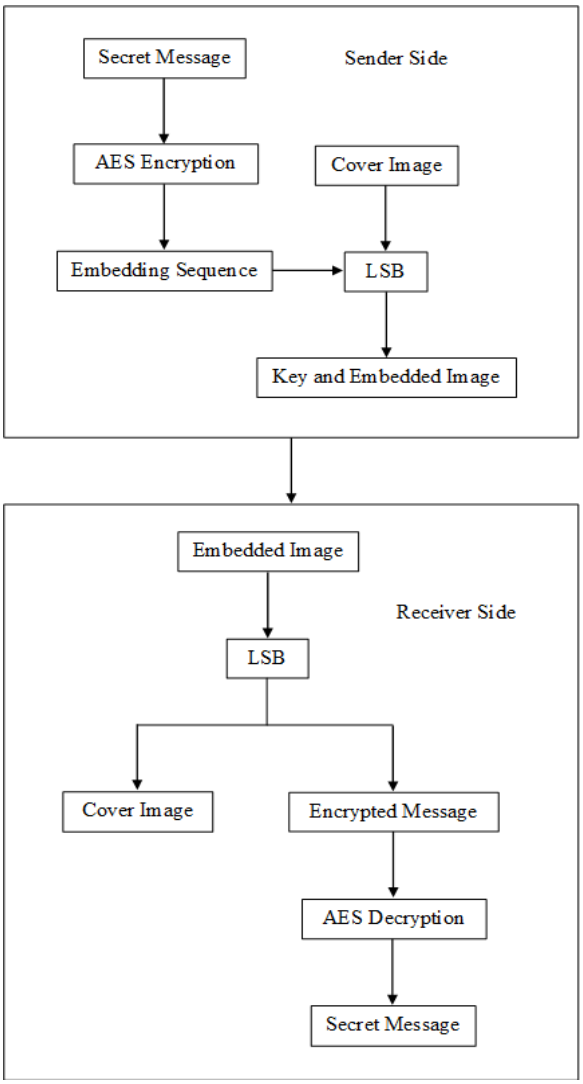

Fig 3.1 System architecture

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

IV.SOFTWARE DESCRIPTION AND INPUTS

ENCRYPTION USING AES

The secret information in text format is encrypted using AES. The message in text format is then converted into ASCII code inorder to convert the text into numbers.The following steps were followed in AES. Thefig 4.1 dsecribes the steps were repeated again and again till the number of rounds.

- Key Generation - key is generated for the secret information depending on its size.
  Instead of giving fixed size key the key is generated based on the size in order to reduce the interaction between the user and the system.
- Add Round Key - The generated key is added to the secret information using bitwise xor operation.
- Sub Bytes - A matrix which is in the size of the column of the secret information is generated and they are referred to as sub bytes. The generated sub bytes were added to the result from the previous step.
- Sift Rows - The rows in the result obtained were shifted left side. The number of shifts is based on the current row of the secret information.
- Mix Columns - The columns in the result obtained were multiplied with the generated sub bytes.

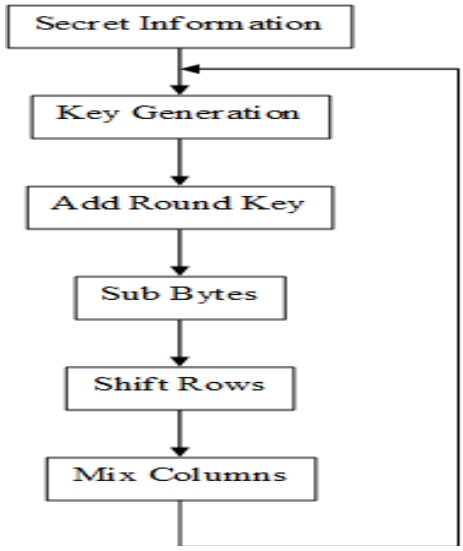

Fig 4.1 AES Rounds

EMBADDING USING LSB

Encrypted secret information is then hided in the input image based on LSB embedding process.In the proposed system, the LSB algorithm is used to hide the encrypted data into the Encrypted image. At the time of steganography separate each pixel RGB bit and then create the 8*8 matrix and calculate the alpha value knows as Complexity.

EXTRACTION USING MSE

At the time of Desteganography we just check the first bit of the 8*8 matrix if it is 0 then we take data as it is. If it's 1 then we EXOR this matrix with the standard chessboard to get the decrypted image.

PERFORMANCES MEASURES

The performance of the process is measured by measuring the PSNR, MSE value.The PSNR and the MSE value shows the similarity between the input secret image and the resulting decrypted image.The PSNR value should be high and the MSE value should be low.

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

Equation 4.1 PSNR

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$ Equation 4.2 MSE

The equation 4.1 and 4.2 descibes to calculating the extraction encrypting image value and comparing the embaddingdecrypting image value.

The Peak Signal to Noise Ratio (PSNR) is the ratio between maximum possible power and corrupting noise that affect representation of image. PSNR is usually expressed as decibel scale. The fig 4.2 PSNR is commonly used as measure of quality reconstruction of image.

The signal in this case is original data and the noise is the error introduced. High value of PSNR indicates the high quality of image.

Mean Square Error can be estimated in one of many ways to quantify the difference between values implied by an estimate and the true quality being certificated. MSE is a risk function corresponding to the expected value of squared error. The MSE is the second moment of error and thus incorporates both the variance of the estimate and its bias.

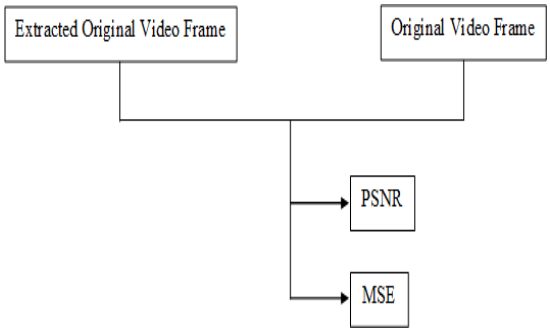

Fig 4.2 Performances Measures process

COMPARISION OF INPUT AND OUTPUT IMAGES OR VIDEO

PSNR	**28.1308**	**28.13**
MSE	**100.008**	**100**
EMBEDDING RATIO	**4**	

V.SOFTWARE DESCRIPTION AND INPUTS

AES ALGORITHM

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 12 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

Byte substitution

The Substitute bytes stage uses an S-box to perform a byte-by-byte substitution of the block. There is a single 8-bit wide S-box used on every byte. This S-box is a permutation of all 256 8-bit values, constructed using a transformation which treats the values as polynomials in $GF(2^8)$ – however it is fixed, so really only need to know the table when implementing. Decryption requires the inverse of the table.

Shift Rows

The Shift Rows stage provides a simple "permutation" of the data, whereas the other steps involve substitutions. Further, since the state is treated as a block of columns, it is this step which provides for diffusion of values between columns. It performs a circular rotate on each row of 0, 1, 2 & 3 places for respective rows. When decrypting it performs the circular shifts in the opposite direction for each row. This row shift moves an individual byte from one

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

column to another, which is a linear distance of a multiple of 4 bytes, and ensures that the 4 bytes of one column are spread out to four different columns.

Mix Columns

The Mix Columns stage is a substitution that makes use of arithmetic over GF(2^8). Each byte of a column is mapped into a new value that is a function of all four bytes in that column. It is designed as a matrix multiplication where each byte is treated as a polynomial in GF(2^8). The inverse used for decryption involves a different set of constants.

Add Round key

Lastly is the Add Round Key stage which is a simple bitwise XOR of the current block with a portion of the expanded key. Note this is the only step which makes use of the key and obscures the result, hence MUST be used at start and end of each round, since otherwise could undo effect of other steps. But the other steps provide confusion/diffusion/non-linearity. That us you can look at the cipher as a series of XOR with key then scramble/permute block repeated. This is efficient and highly secure it is believed.

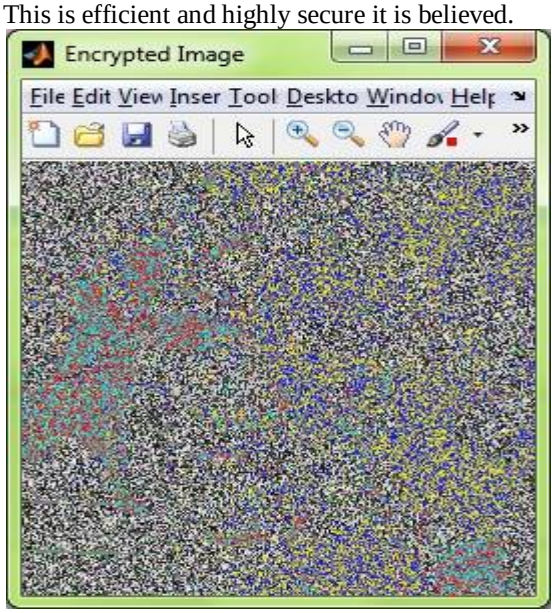

Fig 5.1 Encrypted image

LSB STEGANOGRAPHY

In the first step of LSB steganography the image is split into bit planes. Each bit plane is a binary image which contains the bit of each pixel where 'i' is the plane number. Slicing of planes are represented by a Pure Binary Coding system (PBC) and Canonical Gray Coding system (CGC). Each bit plane can be divided into “informative” and “noise” region. Noise-looking region consist complex pattern and replace each noise looking region with another noise-looking region without changing the overall image quality.

The main goal of LSB Steganography is to increase the capacity of image for data hiding without much distortion in the visual appearance of the original image. The fig 5.2 describes the embedding images using LSB and Pure Binary Coding (PBC) bit planes provides much greater region for embedding. But PBC suffers from “Hamming cliff”, wherein a small change in color affects many bits of color value which can be overcome using CGC in LSB system. The technique of splitting the image into its constituent binary planes is called “Bit plane slicing”.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Fig 5.2 Embedded image

MSB STEGANOGRAPHY

Plane '0' contains all lowest order bits of all pixels in the image while plane '7' contains all higher order bits. Bit plane Slicing is useful for image compression. Complexity of each bit–plane pattern increases from MSB to LSB. In LSB steganography, uncompressed image file is used as carrier image. Each secret file to be embedded is segmented into a series of blocks having 8 bytes of data each which are called as secret blocks. The performance of hiding method was tested using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and embedding capacity of proposed system.

EXTRACTION

The fig 5.3 describes the time of Desteganography we just check the first bit of the 8*8 matrix if it is 0 then we take data as it is. If it's 1 then we EXOR this matrix with the standard chessboard to get the decrypted image.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

5.3 Extracted image

DECRYPTION

The fig 5.4 describes extracted secret information is decrypted based on AES decryption.The methods followed in the AES step is reversed inorder to obtain the secret information.In the first round mix column step is removed. The other steps were reversed.The process is repeated till the number of rounds completed.

Fig 5.4 Decrypted image

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

VI.RESULT AND OUTPUTS

The encryption process is more secure and the information's were well preserved in the image. The embedding ratio is improved.The process is reversible. The distortions will be much reduced in the stego image. Data Security is widely used to ensure security in communication, data storage and transmission. The advantage of LSB-based method is easy to implement and high message pay-load. The fig 6.1 describes the proposed method results is a lossless encryption technique and hence can be widely employed in all the cases. The performance of the process is also much improved.The proposed methodiscompletelyreversible.Thatis, no error happens in data extraction and image recovery steps.The PSNRvalues of marked decrypted image are much higher than those previous methods can achieve under given embedding rates. The extraction anddecryption stepsare independent, which are more natural and applicable.

The LSB steganography are Increased information hiding capacityand Canonical Gray Coded (CGC) bit planes are more are preferred for LSB steganography compared to Pure Binary Coded (PBC) bit planes.The Physical presence of secret information visible by human eyes.

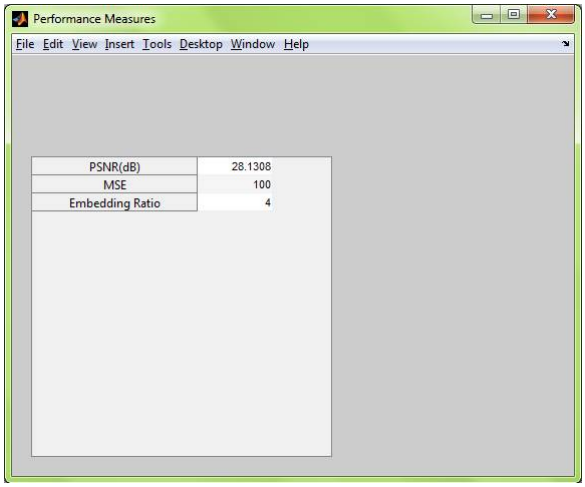

Fig 6.1 Output

VII.CONCLUSION AND FUTURE WORKS

The goal of this project to provide the security of user encrypted messages to hide the LSB embedding images using MATLAB code. Using LSB embedding data is embedding in the identified block. The stego image obtained in this process is forwarded to the receiver. The same process is reversed in the receiver side in order to get the secret information that is hided in the image. The performance of the process is measured with the help of the performance metrics like PSNR, MSE and Embedding ratio. The proposed method performances were much improved compared to the existing methods. In the proposed system, the LSB algorithm is used to hide the encrypted data into the Encrypted image.

REFERENCES

[1] Shivani Khosla1, ParamjeetKaur (2014) Secure Data Hiding Technique Using Video Steganography and Watermarking.
[2] SonaliS.Ekhande Prof. S.P.Sonavane Dr. P .J .Kulkarni (2013) Universal Steganalysis using Feature Selection Strategy for Higher Order Image Statistics.
[3] N. Askari, H.M. Heys, and C.R. Moloney (2013) An extended visual cryptography scheme without pixel expansion for halftone images.
[4] Usha B.A1, N K Srinath2, N K Cauvery3 (2012) Analysis of image steganalysis techniques to defend against statistical attacks .
[5] Ravi Kumar. B #, Murti.P.R.K (2011) Data Security and Authentication Using Steganography .
[6] GurpreetKaur, KamaljeetKaur (2013) Digital Watermarking and Other Data Hiding Techniques Author:
[7] Sandeepkatta (2010) Recursive Information Hiding in Visual Cryptography)

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

[8] G. J. Garateguy, G. R. Arce D. L. Lau (2010) Vonnoi tessellated halftone masks
[9] Isha M. Padiya1, G. D. Dalvi2 (2012) Encrypting Multiple Images Using Visual Secret Sharing Scheme .
[10] Chi-Chen Chang1, Yu-Zheng Wang2 and Chi-Shiang Chan3(2009)An Efficient Probability-based t out of n Secret Image Sharing Scheme.