Reversible data hiding by utilizing AES encryption image & LZW compression

Akshay Kumar Joshi[1], Sanjay Sharma[2]
[1] *Research Scholar in M.tech CSE,* [2] *H.O.D. Dept. of Computer Science, OIST, RGPV, India*

Abstract Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality In this work embedding of data is done applying the LZW algorithm. Then robustness is provide by using the AES algorithm. Finally by using spatial technique embedding of digital data is done in encrypted image. Experiment is done on real dataset image. Evaluation parameter values shows that proposed work has maintain the SNR, PSNR values with high robustness of the data.

Keywords— Reversible data hiding , Digital Watermarking, Frequency domain, AES , LZW..

1. INTRODUCTION

As digital world is growing drastically people are moving towards different services provide by it. Some of this service are social network, online market. But this technology give rise to new problem of piracy or in other words proprietary get easily stolen. In order to overcome this issue many techniques were suggested and proprietary of the digital data is preserved. So to overcome these different techniques are use for preserving the proprietary of the owner. Out of many approaches digital data embedding which is also known as digital watermarking plays an important role. Here digital information is hide in the carrier signal which resembles the originality of the data like photographs, digital music, or digital video [1, 2, 4]. One of the basic cause of the copyright issue is the ease available of the internet and some software that can modify the content as per the user requirement.

In few of approaches inclusion of third party was done by most of the resear3.cher where secret message is hold by one while carrier signal is hold by other [9]. Here embedding is done in fix part of the image where information can be hide. If fit then embedded otherwise reject. Now at extraction side image is evaluate under a calculation where it simply accept or reject image base on the obtain values. Here work has not taken measures for attacks.

Watermark is broadly divide into two category first is visible watermarking and other is invisible watermarking. In case of visible embedding watermark data is open and can be judge by naked eyes. This is shown in fig. 1. On the other hand invisible watermarking is done in such a way that secret information is not seen or judged, so quality of the carrier signal get affected by this. This is shown in fig. 2, although watermark data is present in the original data. Data may be of any digital information like text file, image, video file, etc.

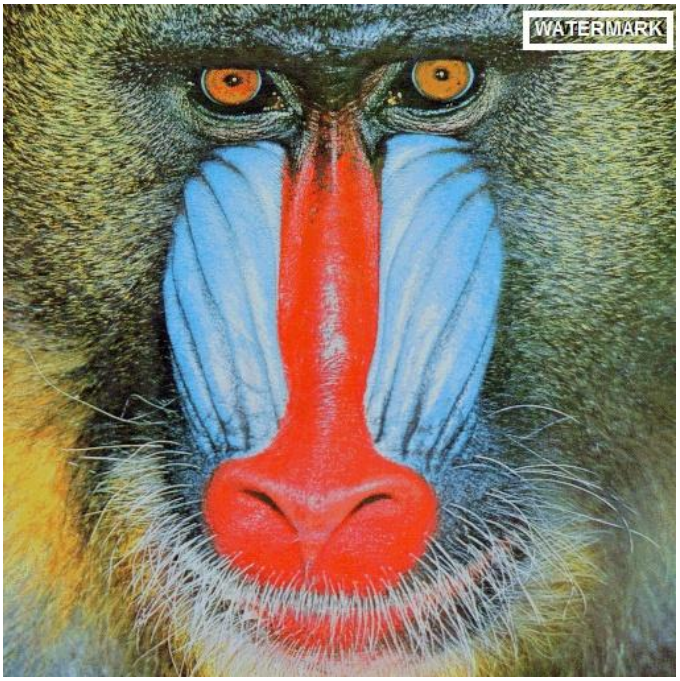

Fig. 1 Visible watermark in image data.

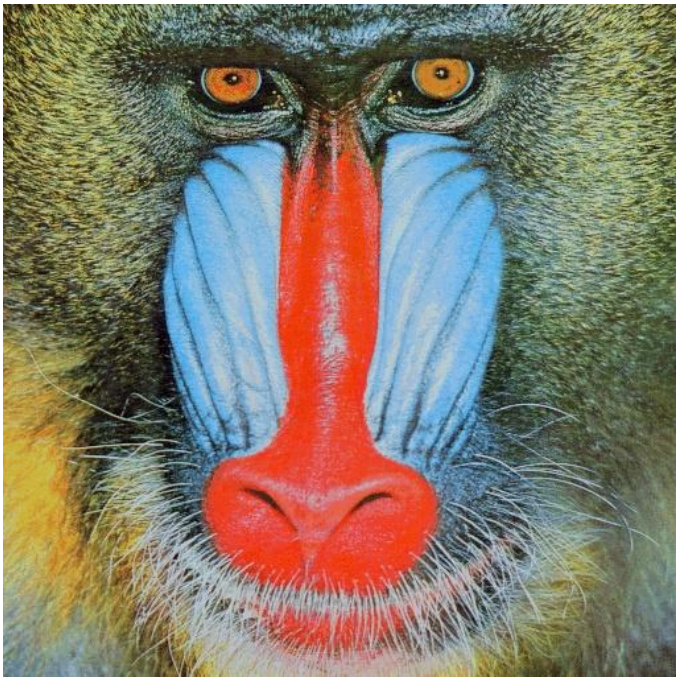

Fig. 2 Visible watermark in image data.

As privacy of digital data is more in case of invisible data hiding technique so popularity of this technique is quit high. As this reduce the chance of copying the watermark as well from the original signal. Although invisible embedding in carrier image is complex and challenging task but different techniques are working in this field.

II. Related Work

In [4] watermark information is hide in the edge portion of the image and for finding the exact egde pixels in the image this paper adopt DAM and BCV technique. Whole work is done for the binary image only as the DAM is base on the binary image. So here in this method image has to be in binary form and watermark information is also in binary format. With this limitation it is found that that robustness of the algorithm is quit good against different attacks of noise, filter.

In [5] the extension of the paper [4] is done where hiding is done at the edge region only using same technique of DAM and BCV but here edge selecting region is increase by searching surrounding region of the evaluating pixel. It has shown in the result that with this new approach robustness increases and the watermark information can be increase in the original image.

In [7] new concept is develop by the paper which is term as content reconstruction using self embedding, here watermark image is embedded in the original image using fountain coding algorithm, where multiple packets are designed for the network. So if some of the packet get corrupt by the attack then rest of the packets are use for regenerating the original watermark. As this method cover different attacks on the image and recover watermark in original condition upto few level of attack. One problem is that after embedding image get transformed in fountain codes packet but embedded image is not available for the user to display and it get reconstruct into original only by decoding the fountain codes. So this algorithm is beneficial for data transferring purpose only.

In [6] instead of embedding the external watermark image, original image is so utilize in the algorithm that it will generate its own watermark bits for the image. This paper focus on the image expansion where spatial domain is use for embedding and supporting information is store for the image which is required during extraction. Robustness of the image is done against compression attack and scaling is also cover.

But to cover both intra-code block and inter-code block method is utilize.

In [12] during embedding the algorithm uses DWT technique and modulus method for the pixel position selection. At the extraction end embedded image with some supporting information is supply for generating the original image and watermark bits. This recovery of original watermark is reversible watermarking scheme.

In [8] K-SVD is adopt as the trainer. For the room preserved self embedded image generate the encrypted image Ie by a stream cipher, such as RC4. Data Hiding in Encrypted Images : Once the encrypted image is received, the data hider can embed secret data for management or authentication requirement. The embedding process starts with locating the encrypted version of area. Since the image owner has embedded the position of the first room preserving patch and the room size for each patch in the encrypted image, it is effortless for the data hider to know where and how many bits they can modify.

III. Proposed Methodology

This paper focus on the digital image data hiding techniques. Then two steps are explained first is embedding and other is extraction In case of extraction watermark should be successfully retrieve from the received data without any information loss of the original data as well as watermark [7, 8]. In Fig. 3 whole embedding work block diagram is explained.

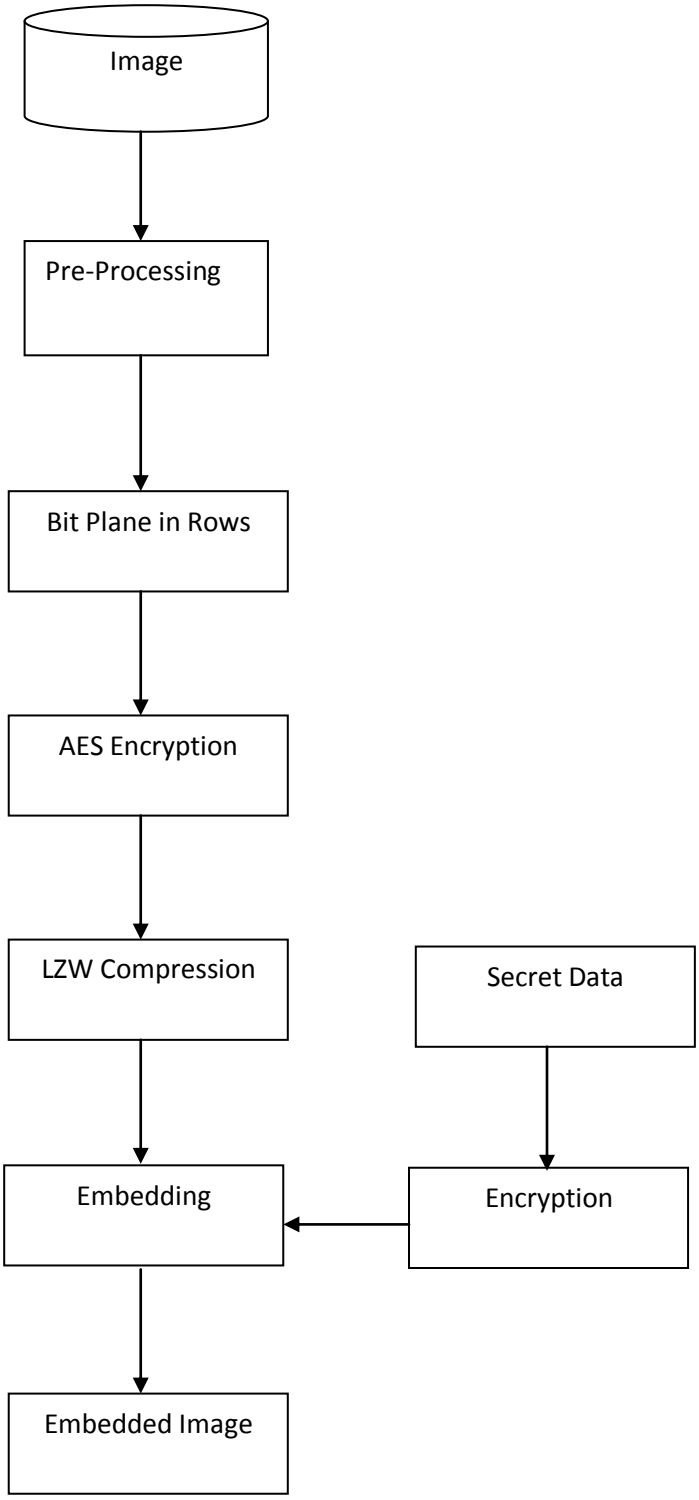

Fig.3 Block diagram of proposed work.

Pre-Processing

Here as the image is the collection of pixels where each pixel is representing a number that is reflecting a number over there now for each number depend on the format it has its range such that for the gray scale format it is in the range of 0-255. So read a image means making a matrix of the same. dimension of the image then fill the matrix correspond to the pixel value of the image at the cell in the matrix

Bit Plane in Rows

In this step all the color channels Red, Green and Blue are divide into row wise as per the there matrix. Now each row is convert into its equivalent binary value. As single vector was create in this work for each row, so pixel value of each color channel is consecutive to the pixel value of same row in the same color channel.

AES

In this encryption algorithm four stages are perform in each round. These steps are common in both encryption as well as decryption algorithm where decryption algorithm is inverse of the encryption one. Now common step for all kind of data is that each data need to be convert into 16 element set of input. Here each input need to be in integer data type. So round consist of following four stages.

- Byte substitution (1 S-box used on every byte)
- Shift rows (permute bytes between groups/columns)
- Mix columns (subs using matrix multiply of groups)
- Add round key (XOR state with key material)

LZW Compression

In this technique trick is that string-to-codeword mapping is created dynamically by the encoder also recreated dynamically by the decoder need not pass the code table between the two is a lossless compression algorithm degree of compression hard to predict depends on data, but gets better as codeword table contains more strings.

step 1. Initialize table with single character strings
step 2. STRING = first input character
step 3. WHILE not end of input stream
  a. CHARACTER = next input character
  b. IF STRING + CHARACTER is in the string table
    i. STRING = STRING + CHARACTER
  c. ELSE
    i. Output the code for STRING
    ii. Add STRING + CHARACTER to the string table
    iii. STRING = CHARACTER
step 4. END WHILE
step 5. Output code for string

Embedding of Secret data

In this section data hiding is done in the compressed image. Here as each image row is compressed, so rest of the blank portion of the row is used for data hiding. So blank portion of the data can be replace with hiding data. In this way hiding of data was done.

Extraction steps

In this extraction steps receiver can extract data and image by using above block diagram.

LZW De-Compression

step 1. Initialize table with single character strings
step 2. OLD = first input code
step 3. output translation of OLD
step 4. WHILE not end of input stream
  a. NEW = next input code
  b. IF NEW is not in the string table
    S = translation of OLD
    S = S + C
  step 5. ELSE
    S=translation of NEW
  c. EndIF
  d. output S
  e. C = first character of S
  f. OLD + C to the string table
  g. OLD = NEW
step 6. END WHILE

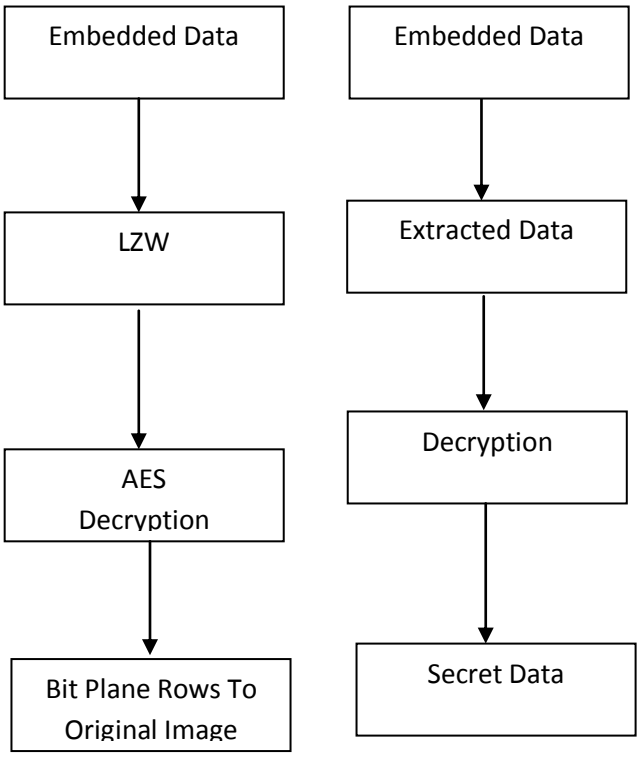

Fig.4 Block diagram of data extraction at receiver end where (a) represent extraction of original image while (b) represent extraction of original data.

Extraction of Image

This section of proposed work is for image extraction at receiver side. Here first LZW compressed data was extract from the packet. In order to differentiate image values and hiding data in the packet, zero is used as a separator. So values before 0 is consider as the image data. Now this image data is first de-compress by LZW algorithm. So resultant series is row of cover image. In similar fashion all the rows is extract from the compressed data files.

Now all extracted value in form of row is decrypt by AES algorithm having same key values. In this way all the plane in form of rows are combine to make single image for output of the image.

Extraction of Data

This section of proposed work is for data extraction at receiver side. Here first embedded data was extract from the packet. In order to differentiate image values and hiding data in the packet, zero is used as a separator. So values after 0 is consider as the image data. Now all extracted value is decrypt by AES algorithm having same key values. Now ASCII values are convert into corresponding characters.

IV. Experiment and Result

This section presents the experimental evaluation of the proposed Embedding and Extraction technique for privacy of image. All algorithms and utility measures were implemented using the MATLAB tool. The tests were performed on an 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM, and running under Windows 7 Professional.

Dataset: Experiment done on the standard images such as mandrilla, lena, tree, etc. These are standard images which are derived from http://sipi.usc.edu/database/?volume=misc. System is tested on day to day images as well.

Original Image		
		

Table 1 Dataset representation.

Evaluation Parameter:

Peak Signal to Noise Ratio

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Signal to Noise Ratio

$$\text{SNR} = 10\log_{10}\left(\frac{Signal}{Noise}\right)$$

Extraction Rate

$$\eta = \frac{n_c}{n_a} \times 100$$

Here n_c is number of pixels which are true.

Here n_a is total number of pixels present in watermark.

Results:

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	35.5347	9.3743
Tree	34.3451	10.425
Lena	32.09	9.2113

Table 2. PSNR Based Comparison between proposed and previous work.

From table 2 it is obtained that proposed work is better as compare to previous work in [8]. under PSNR evaluation parameters. As compression algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

SNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	16.3864	2.46871
Tree	16.8352	2.4174
Lena	16.293	2.63165

Table 3. SNR Based Comparison between proposed and previous work.

From table 3 it is obtained proposed work is better as compare to previous work in [8]. under SNR evaluation parameters. As compression algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Extraction Rate Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	100	100
Tree	100	100
Lena	100	100

Table 4. Extraction rate Based Comparison between proposed and previous work.

From table 4 it is obtained that proposed work is better as compare to previous work in [8]. under Extraction rate evaluation parameters. As compression algorithm performs well in order to compress the image highly and generates more space for hiding of secret data.

Execution Time Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	27.6171	54.8
Tree	30.7853	55.5632
Lena	28.6011	58.263

Table 5. Execution time Based Comparison between proposed and previous work.

From table 5 it is obtained that proposed work is better as compare to previous work in [8]. under execution time evaluation parameters. As proposed work regenerate dictionary from the same data so execution time for the same is less as compare to previous work.

Hiding capacity Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	5120	6413
Tree	5120	6042
Lena	5120	6219

Table 6. Hiding capacity Based Comparison between proposed and previous work.

From table 6 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under hiding position evaluation parameters.

V. CONCLUSION

Here proposed work has efficiently embedded data in the carrier image while security of the carrier is also maintained by encrypting using AES algorithm. Embedding is done in LSB position of the pixel values. Proposed algorithm will recover or reverse complete data at receiver end. Results shows that the proposed work is producing the results which maintain the image quality as well as robustness. In future, work can be improve for other attacks such as geometry of image.

VI. REFRENCES

1. Tamanna Tabassum, S.M. Mohidul Islam "A Digital Image Watermarking Technique Based On Identical Frame Extraction In 3-Level DWT" Vol. 13, No. 7, Pp. 560 –576, July 2003.

2. Frank Hartung, Jonathan K. Su, And Bernd Girod "Spread Spectrum Watermarking: Malicious Attacks And Counterattacks". Of Multimedia Contents" International Journal Of Research In Engineering And Technology Eissn: 2319-1163 | Pissn: 2321-7308, 2005.

3. "CHAPTER 2. WAVELET TRANSFORMS ON IMAGES" *Sundoc.Bibliothek.Uni-Halle.De/Diss-Online/02/03H033/T4.Pdf, 2008.*

4. Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ And Shigeo Kato . "Digital Image Watermarking Method Using Between-Class Variance". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

5. Angela Piper1, Reihaneh Safavi-Naini. "Scalable Fragile Watermarking For Image Authentication". Published In IET Information Security, On 31st December 2012

6. Mr Mohan A Chimanna 1,Prof.S.R.Kho "Digital Video Watermarking Techniques For Secure Multimedia Creation And Delivery" Vol. 3, Issue 2, March -April 2013, Pp.839-844839.

7. Paweł Korus, Student Member, IEEE, And Andrzej Dziech. "Efficient Method For Content Reconstruction with Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.

8. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo High Capacity Reversible Data Hiding In Encrypted Images

By Patch-Level Sparse Representation. IEEE TRANSACTIONS ON CYBERNETICS 2015.

9. Hanieh Khalilian, Student Member, IEEE, And Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" Ieee Transactions On Image Processing, Vol. 22, No. 12, December 2013.

10. Shahzad Alam, Vipin Kumar, Waseem A Siddiqui And Musheer Ahmad. 2 "Key Dependent Image Steganography Using Edge Detection". Fourth International Conference On Advanced Computing & Communication Technologies 2014.

11. Ioan-Catalin Dragoi, Member, IEEE, And Dinu Coltuc . "Local-Prediction-Based Difference Expansion Reversible Watermarking" . Ieee Transactions On Image Processing, Vol. 23, No. 4, April 2014.