Reversible Data Hiding by Utilizing AES Encryption and LZW Compression

Akshay Kumar Joshi[1] , Sanjay Sharma[2]

[1]*Research Scholar, M.Tech. in CSE* , [2]*Associate Professor. Dept. of Computer Science, OIST, RGPV, India*

Abstract ***Recently, very much attention is paid to reversible hiding (RDH) scheme in ciphered images, since it maintains the good property that the real cover can be restored after embedded data is extracted while providing privacy to the cover image. This work embedding of data is done applying the LZW compression algorithm. Then robustness is provide by using the AES Advance encryption standard 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.

I. 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 this 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.

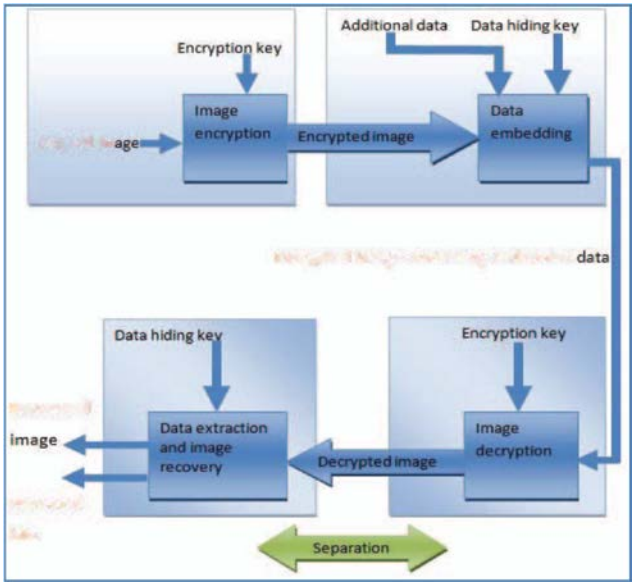


Figure1 Reversible data hiding scheme.

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.

The term "reversible data hiding" means getting the exact recovery of the data after performing the process like encryption-decryption and data hiding.

II. RELATED WORK

In [5] author has extend the work done in [4] by increasing the overall capacity of the embedding data space. Here in Dam and BCV technique author start looking at the surrounding of the edge region pixel. So overall capacity of the data hiding was drastically increase in this paper. Here even after embedding more data embedded image was robust against different type of attack as well.

In [7] self embedding concept was proposed by the authors where image itself generate the data for embedding while in order to protect data in network fountain codes were developed for lost packed regeneration. As in fountain codes more than one required packet format was send in the network, which help in regenerating the missed or corrupt data packets. Here work has great limitation was that after embedding the image is not available in original format before extraction. So main purpose of this work is for transferring the data packet from sender to receiver only.

In [6] same concept of image watermark self generation was done, here image was so utilize that it generate its own watermark information. This paper focus on the image development where spatial area was utilize for inserting the digital data as a carrier object. At the same time similar information is required at the receiver which help in finding the digital data back. But to cover both intra-codeblock and inter-codeblock method is utilize.

In [8] author adopt KSVD technique for embedding the digital data. Here by utilizing the DES algorithm encryption of the digital data was done. Here one dictionary was maintained at the receiver and transmitter end for reducing the size of carrier signal. In this work after embedding some vacnt space between the data was utilize for the data embedding. This work has give freedom for extraction of image or digital data or both in any order.

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. In Fig. 3 whole embedding work block diagram is explained.

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

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. 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.

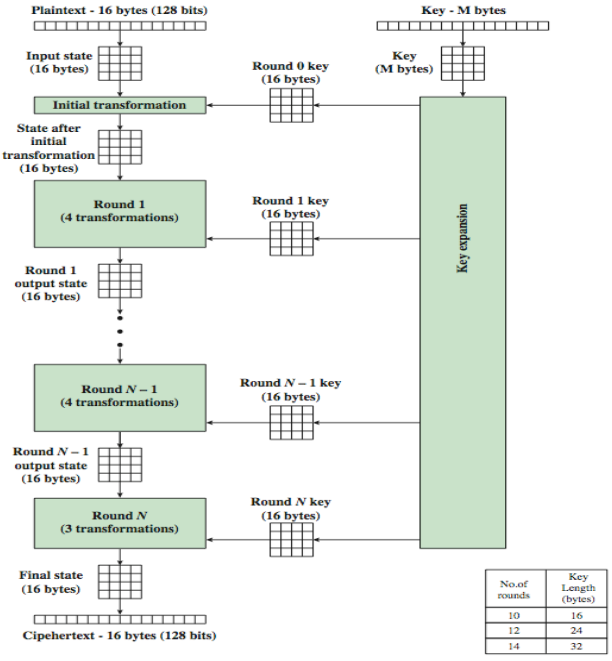


Figure 2 AES encryption system.

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)

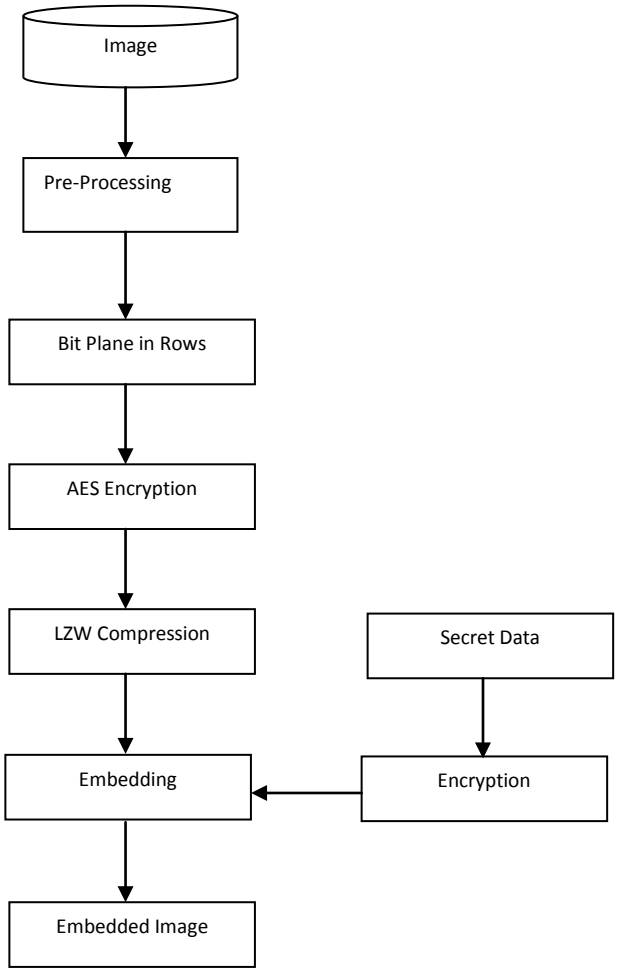


Fig.3 Block diagram of proposed work.

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

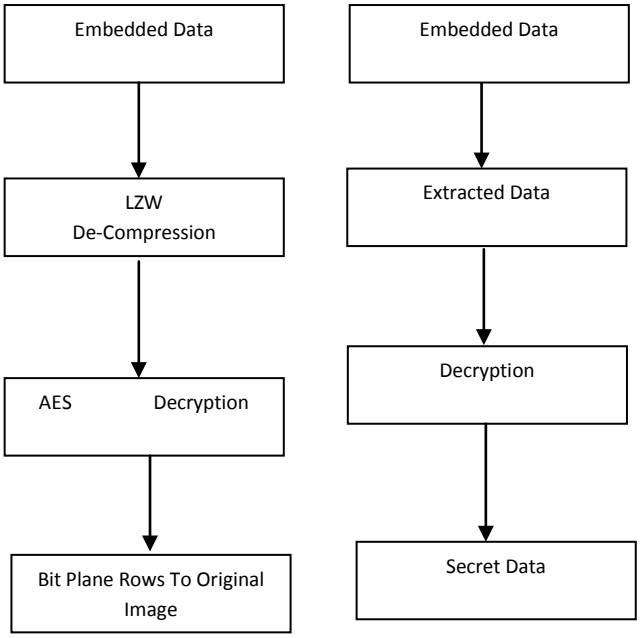
In this section data hiding is done in the compressed image. Here as each image row is compressed, so rest of the blank portion of the row is used for data hiding. So blank portion of the data can be replace with hiding data. In this way hiding of data was done.

Extraction steps

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

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



(a) (b)

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

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.

ALGORITHM

Input: CI (Cover Image), HD (Hiding Data)

Output: EP (Embedded Packet)

- CI←Pre-Processing(CI)
- Loop 1:3 // for Each C (Channel) {Red, Green, Blue}
- C←CI
- Loop 1:n // n : number of row in channel C
- R←C[n]
- ER←AES_Encryption(R) // ER: Encrypted Row
- CR←LZW_Compression(ER) // CR: Compressed Row
- P←CR // P packet
- EndLoop
- EndLoop
- While P is blank AND count <=:m // m number of characters in hiding data
- EHD ←AES encryption(HD) //EHD : Encrypted hiding data
- EP←EHD[count] //EP : Embedded Packet
- count = count+1
- End While

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 converted into corresponding characters.

IV. EXPERIMENT AND RESULT

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

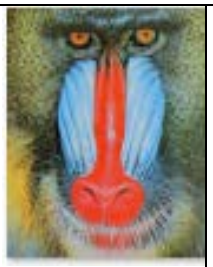
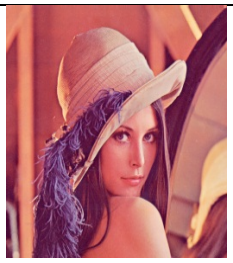
Original Image		
		

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

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

Results:

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	39.5347	29.3743
Tree	38.3451	30.425
Lena	37.09	29.2113

Table2. 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.

From table 3 it is obtained proposed work is better as compare to previous work in [8]. under SNR evaluation parameters.

SNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	26.3864	17.46871
Tree	26.8352	18.4174
Lena	24.293	16.63165

Table3. SNR Based Comparison between proposed and previous work.

As proposed work regenerate dictionary from the same data so execution time for the same is less as compare to previous work.

Execution Time Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	27.6171	54.8
Tree	35.7853	50.5632
Lena	32.6011	49.263

Table5. 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.

Hiding capacity Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	6420	5413
Tree	6120	5042
Lena	6052	5219

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

In our work, we have developed a new technique for reversible data hiding in Digital color images. The cover image is first encrypted and compressed by AES encryption and LZW compression respectively and then encrypted secret message is embedded in it. This work in RDH solves the problem of less embedding capacity. The results show that embedding capacity compared with existing approaches is more while maintaining the quality.

Also higher PSNR of the decrypted cover image is observed after performing encryption-decryption, data hiding and data extracting process on cover image

VI. REFERENCES

[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.