Reversible Data Hiding For Image with Contrast Enhancement and Video Using Encryption and Decryption

Asha S Raj, Gayathri Nair P

Abstract— The Reversible Data Hiding is a widely used technique. The host image can be recovered exactly. Reversible Image Data Hiding Using Encryption and Decryption with Contrast Enhancement. It is applied at medical and military applications. The data embedding process will usually introduce the continuous loss to the cover image. In several areas such as medical, military, and law forensics degradation of cover image is not allowed. For the sake of Reversible Image Data Hiding Using Encryption and Decryption with Contrast Enhancement. The main applications are medical and military areas. The digital images that embeds data into image. It alters the pixel values for secret communication. The cover image can be retrieved to its original state after the extraction. Reversible Image Data Hiding Using Encryption and Decryption for high security and efficiency. It enables images to data in hidden format. The restored images into their origin by removing digital hidden data. The Reversible Image Data Hiding Using Encryption and Decryption with Contrast Enhancement which uses the encryption and decryption for enhancing the security of the whole system.

Index Terms— Reversible Data Hiding, PSNR, RDH, HE, Difference expansion (DE), XOR Encryption, XOR Decryption

1 INTRODUCTION

A reversible data hiding is used to recover the original image without any distortion. Reverse the data from the marked image. When the hidden data have been separated [1]. The method utilizes the zero or the minimum points. The points of the histogram of an image can be used for reversing. It modifies the pixel values to embed data into the image. It is used to embed more data. One of the many existing reversible data hiding techniques are used. It is the peak signal to noise ratio (PSNR) of the marked image. The PSNR generated by the method for the easy calculation. The PSNR is higher value for all reversible data hiding techniques. It is used to embed a piece of information into the host images to generate the marked one. The techniques utilizes the zero or the minimum points are used.

The original image can be exactly recovered. After extracting the embedded data from the marked one. The original image can be processed. It get the reversed image of the original one. One of the many existing reversible data hiding techniques are used. It is the peak signal to noise ratio. After the embedded information is separated. The Reversible Data Hiding process eliminates the disadvantages of reverse process in watermarking. The process to invert the output images back to the original images . When the hidden data are separated. The process is to be used the Peak Signal Noise Ratio (PSNR) to check the quality of reversed image.

The PSNR range is the utmost possible power of a signal and the power of perverting noise. It is the most commonly used method. The measure of0 quality of reconstruction. Peak Signal Noise Ratio represents the deformity level between output image and input image. Reversible Data Hiding is used Difference expansion (DE) [2]. It is one of the most important approaches. These techniques are used for reversible data hiding. The help of PSNR value the recovered images can be examined.

Reversible data hiding is used for embedding information into input such as image, audio, and video files. It can be applied for media notation, copyright protection etc. The data hiding methods embed messages into the input images. The original image moved into the data hiding process . The output images get the reversed image. The modified part of the cover image is least significant part. The embedding process will usually introduce continuous distortion in original image. The original cover image is never be reconstructed image. From the marked cover image the original image can be retrieved. The main areas are medical imagery, military imagery, and law forensics. The original image is not undergoes any degradation allowed. It need a different type of data hiding method. Which is reversible data hiding (RDH) or lossless data hiding [3]. The original cover image can be reversibly restored after the embedded message is separated.

Reversible data hiding that embeds more important data into images, audio, video etc. Source side the data is embedded by the reversible manner. The destination side the data is separated by the converse manner. Once the secret data are embedded in the compression sector side. The destination stores the input image in a compression side to save storage area. The output is used to extract the secret data to reconstruct the input image. Then cram the input image again to generate compression codes.

Reversible data hiding in all the images is a new method. Be-

cause of the privacy preserving from cloud data which are used the RDH. The methods implement RDH in encrypted images. By encryption and decryption used in the data hiding method [8]. The proposed by reserving pixel before encryption. The data hidden is the benefit from the retrieved data. The previous step to make data hiding process very easy. The proposed method can take advantage of all previous RDH techniques. For plain images and getting an excellent performance. The previous RDH techniques are used. For encrypted and decrypted the image are used for the processing. The degradation of perfect data hiding data is used [9]. The novel method can getting real reversibility. Separate data extraction and more improved on the quality of decrypted images. The previous RDH techniques are used. For encrypted and decrypted the image are used for the processing. The previous step to make data hiding process very easy. The proposed method can take advantage of all previous RDH techniques. For plain images and getting an excellent performance.

The process used the reversible data hiding using encryption and decryption of images. The algorithm is based on Ceaser Cipher algorithm [7]. The random generation process can be used. The concept of shuffling the rows in the pixels of data. That is rows transposition and Huffman Encoding are used. Encryption and Decryption of an image by this algorithm protect the image from an unauthorized accessing method. The Algorithm provides high security to an image. And the process occupy minimum memory area. The data embedding process is used. By using the Integer Wavelet Transform for the process. It can reduce the mean square distortion between the original and watermarked image. And also to increase Peak signal to noise ratio [12]. Also all the experiments are done in the gray scale images.

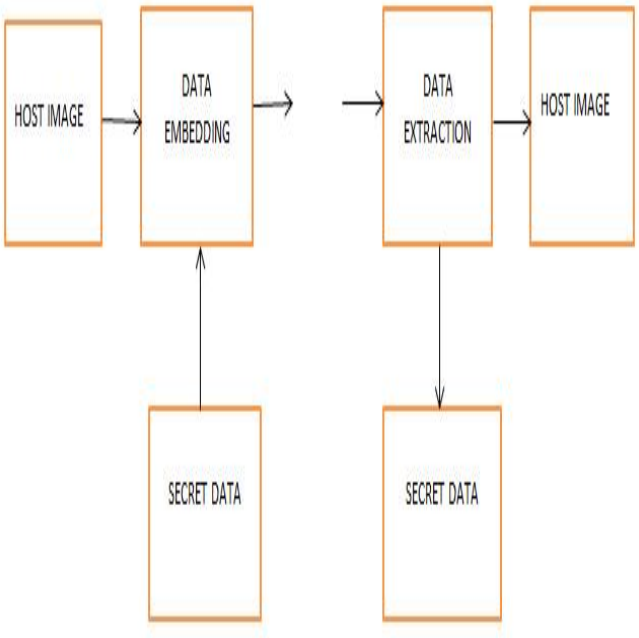


Fig 1. Reversible data hiding

The method also used in color images. A new reversible data hiding techniques has been developed. The property of contrast enhancement is used for more brighter pixels. The two peak values in the histogram are selected for data embedding. The histogram equalization can be performed by replicated the techniques. The results that the image contrasts can be enhanced by splitting a number of histogram peaks. the pixel peaks to be splitted pair by pair. The enhanced contrast enhancement can be used in the proposed method. The 2 peaks in the histogram can be calculated from the pixel values of the given images. The RDH which providing more security with the help of XOR-Encryption and XOR-Decryption techniques [6]. XOR-Encryption which encrypt the data with high security and the reverse process done in the side of XOR-Decryption [7].

The PSNR [4] of a marked image generated with a predicted error. Based on the algorithm which is high . The visual quality can easily be improved. Because more degradation of data is introduced by the embedding operations. For the images acquired with poor illumination rate. The improving visual quality is more important than keeping the PSNR [4] value high. The contrast enhancement of medical or satellite images is used to present the features for visual observation method. The PSNR [4] value of the enhanced image is represented low. Once the secret data are embedded in the compression domain mode. The receiver store the cover image in a compression mode to save storage space. The output is used to extract the secret data to reconstruct the cover image. The visibility of image details has been improved. To the best idea there is no existing RDH algorithm to performs the function of contrast enhancement.

2 RDH USING ENCRYPTION AND DECRYPTION WITH CONTRAST ENHANCEMENT

2.1 Data Embedding by Histogram Modification

The Data embedding section is used for embedding the data or the image into the host image. The color images can be converted into the gray level images. The gray level images represented into the pixel format. The 8-bit gray level image denoted by I. The visual quality can easily be improved. Because more or less distortion has been introduced by the embedding operations. For the images getting with less illumination rate. The histogram can be calculated by counting the pixel with a gray level value represented j. Use hi to denote the image histogram so that hi(j) denotes the number of pixels with value j. Then non empty bins in the histogram are denoted hi. From the hi the two peaks (i.e. the highest two bins) are selected. The denoted smaller and bigger values are denoted by and respectively.

2.2 Pre-Process for Complete Recovery.

In the RDH algorithm, it is used that all pixels counted in hi are {1,…,254} . If the pixel having any bounding pixel value (0 or 255). The overflow or underflow problem will be caused by

histogram shifting. The gray level images represented into the pixel format. The 8-bit gray level image denoted by I. The visual quality can easily be improved. Because more or less degradation has been generated by the embedding operations. To avoid this problem the histogram needs to be preprocessing. The histogram modification operations are pixel modifications. The pixel values of 0 and 255 are changed to 1 and 254. Because overflow or underflow will be caused because the possible change of all pixel is ± 1 . To remember the pre-processed pixels of the image. The location map with the same size as the original image is obtained. By giving 1 to the location of a modified pixel. And 0 to that of an unchanged one (including the 16 excluded pixels). The location map can be pre-computed. Then they given by the binary values to be hidden. In the extraction and recovery process can be done. It can be obtained from the data extracted. The marked image so that the pixels changed in the pre -process can be reported. By restoring the original values of those pixels. The original image can be completely recovered.

2.3 Encryption

XOR encryption (or Exclusive-OR encryption) [5] is a common method. It encrypting text into a format that cannot be easily identified by the average person. XOR decryption (or Exclusive-OR encryption) is a common method of decrypting text into a format that cannot be easily identified by the average person. Secure or insecure XOR encryption is used in the RDH algorithm. It has no of valid use cases [7]. To the best plan there is no already used RDH algorithm that implement the function of contrast enhancement. XOR encryption is great for storing things. It like game save data, and other data types that are stored on a user computer. That cannot a big task. XOR encryption [6] is also used as a part of more complex encryption algorithms. Which are the game save data, and other data types that are stored locally on a user computer. The notations (JSON uses '{' and '}' characters, XML contains wealth of '<' and '>' characters, etc.) are used to be encryption and decryption. So if someone is able to determine the pattern. And open even one character. It uses the key to open everything else.

2.4 Contrast Enhancement

The two peaks in the histogram is split into two nearest bins. With the same or equal heights are used. Because the To increase the data embedding rate the highest two bins in the modified histogram are further chosen to be split. To all pixels arranged in the histogram with order. The identical process can be repeated by separated each of the two peaks. The pixels into two nearest bins with the identical heights. To achieve the Histogram Equalization (HE) effect [11]. Data embedding and contrast enhancement are together performed. The peak pair number of the histogram peaks to be split is L, the range of pixel values from 0 to L-1 are added by L then the pixels from 256-1 to 255 are subtracted by L in the preprocess (representing L is a positive integer). A location map is giving by assigning 1s to the changed pixels, and 0s to the others.

Secure or insecure XOR encryption is used in the RDH algorithm. It has no of valid use cases [7]. To the best idea there is no already used RDH algorithm that performs the task of contrast enhancement. XOR encryption is great for storing things. XOR encryption is great for storing things. It like game save data, and other data types that are stored on a user computer. That cannot a big process. XOR encryption [6] is also used as a part of more complex encryption algorithms. Which are the game save data, and other data types that are stored locally on a user computer.

2.5 Decryption

XOR decryption (or Exclusive-OR decryption) is a common method of decrypting text into a format that cannot be identified and detected by the average person [7]. XOR decryption (or Exclusive-OR decryption) is a used method. The decrypting text into a format that cannot be detected by the average person. XOR decryption is commonly used for storing function. XOR decryption is also used as a part of the decryption algorithms. The applications are game save data, and other data types that are stored locally on a user computer.

The idea behind it is that if you don't know the original character or the XOR decryption key. It is impossible to determine which is used for the data hiding. The reason that it is not completely secure. It is used the data almost always contains patterns, characters, XML contains no of notations '<' and '>' characters, etc.). So if someone is able to determine the pattern. It unlock even one character. It will have the key to unlocking the whole process. The use of XOR encryption to store the antivirus, web filters, and even researchers. It has been used for many years. While it is better encryption algorithms. The XOR cipher is very easy to add to a project. It is low capital and is little effective today.

- **First Author name** , **Asha S Raj**, P G Scholar, Mohandas College ofEngineeringandTechnology,Thiruvananthapuram,Kerala,India (e-mail:symashasraaj@gamil.com).
- **Second Author name**, **Gayathri Nair P**, Assi. Professor, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India (e-mail: gayathrinp2010@gmail.com).

The location map is to be pre calculated. And the location map going to be compressed. With the last two peaks to be split for embedding. Whose values are stored in the LSBs of the 16 excluded pixels. To be embedded into the host image. The rate of the L, the size of the compressed location map are used. And the previous peak values in the pixels are embedded. With the last two peaks to be split for embedding. Whose values are stored in the LSBs of the 16 prohibited pixels. In the separation techniques the last split peak values are retrieved. And the data embedded with pixels are separated. After restoring the histogram data embedded with the previously split peak. It can also be separated. By processing the pair by pair of pixels. At last, the location map is obtained from the separated data. To identify the pixel ranges modified in the preprocess.

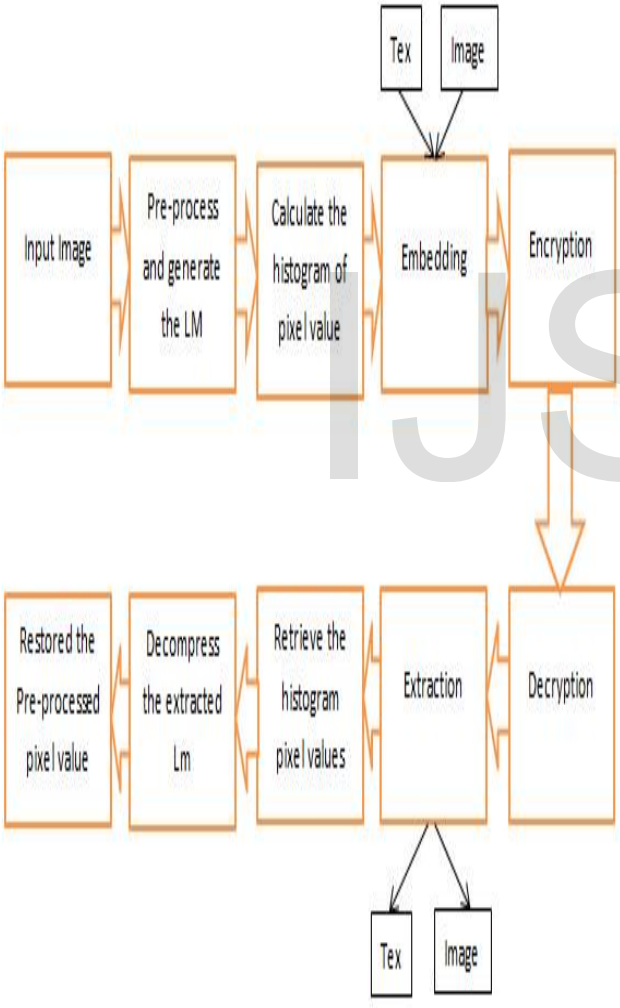


Fig 2. The Reversible Data Hiding Using Encryption and Decryption with Contrast Enhancement

3 EXPERIMENTAL RESULTS

3.1 IMAGE HIDING

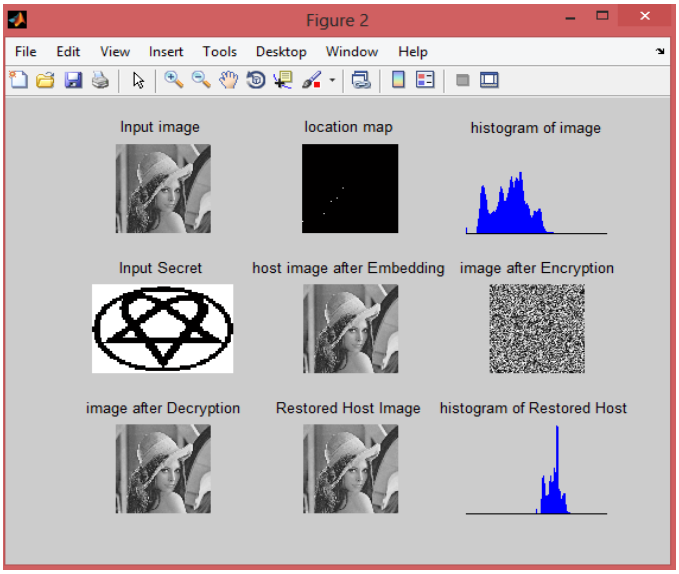


Fig 3.1 (a). Image Hiding Output

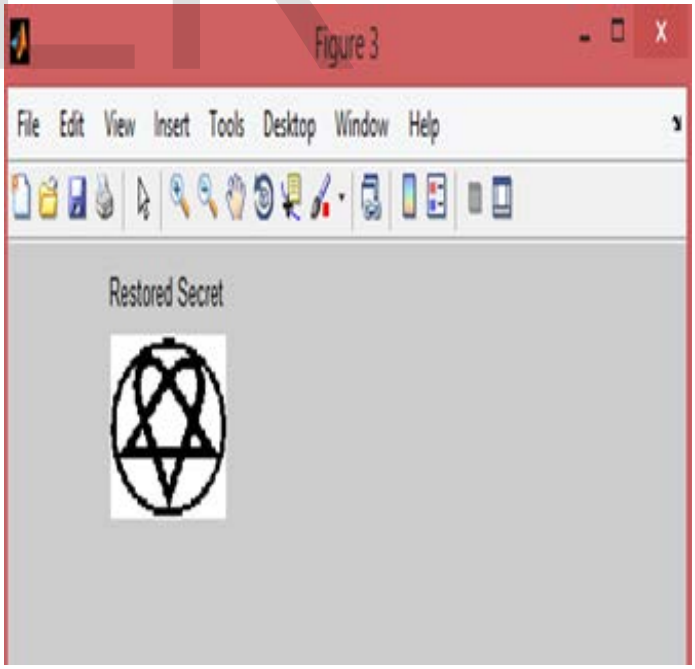


Fig 3 (b). Image Hiding Output

The Fig III (a) and Fig III (b) shows the output of image hiding

techniques. The proposed method can take advantage of all previous RDH techniques. Respected output has been shown after fulfilling respective needs.

3.2 TEXT HIDING

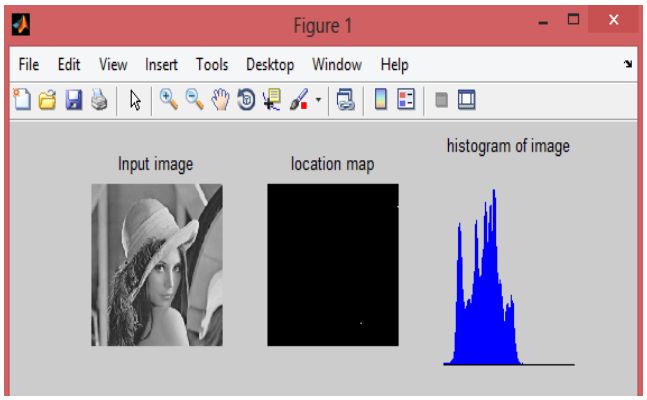
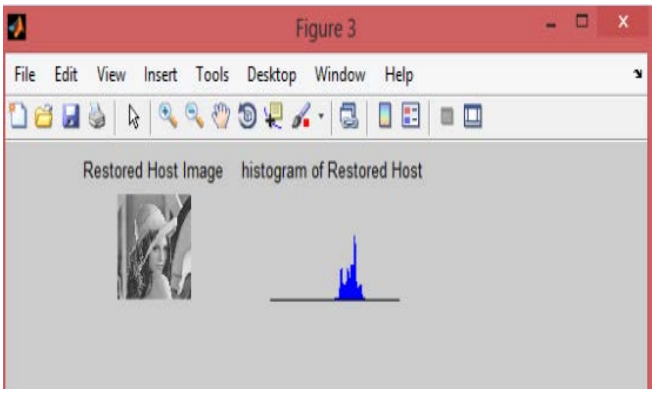


Fig 3.2 (a). Text Hiding Output

Fig 3.2 (b). Text Hiding Output



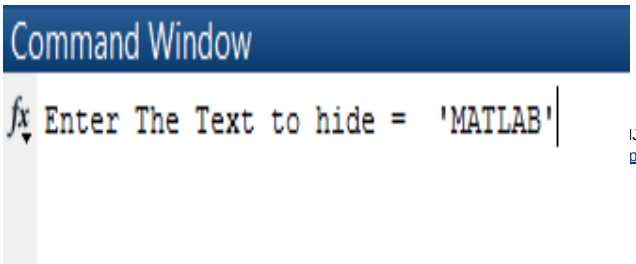


Fig 3.2 (c). Text Hiding Output

Fig 3.2 (d). Text Hiding Output

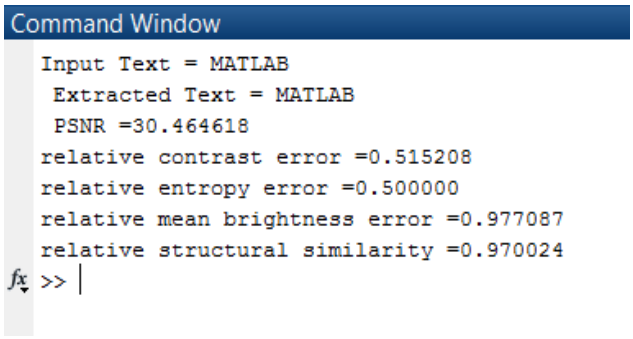


Fig 3.2 (e). Text Hiding Output

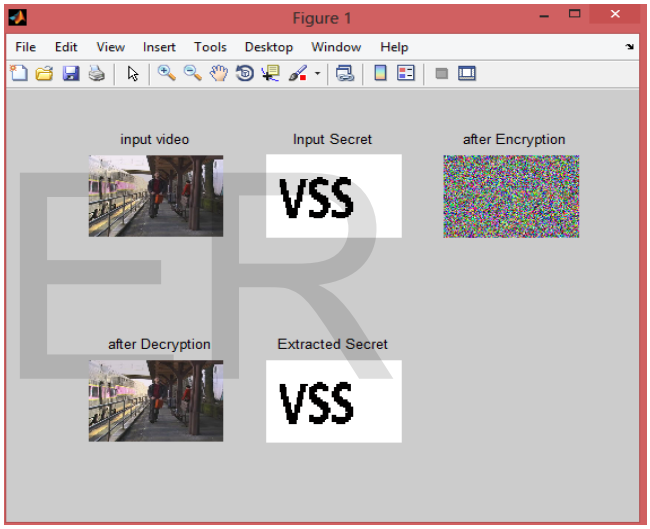


Fig 3.2 (f). Image Hiding (video) Output

Fig 3.1 (a), (b), 3.2 (a), (b), (c), (d) and (e) Above mention figures represents Text Hiding techniques proving the respective outputs. Fig 3.2 (f) figure represents the image hiding output of video. Respected output has been shown after fulfilling respectively needs.

4 RESULT ANALYSIS

SI.NO	NAME OF THE IMAGE	PSNR OF INPUT IMAGE	PSNR OF OUTPUT IMAGE
1	Lena	33.867	33.867
2	Gold hill	32.323	32.323
3	Tank	33.872	33.872
4	Monkey	30.606	30.606
5	Nature	31.876	31.876
6	Rail	32.873	32.873
7	Flower	30.123	30.123
8	PC	32.012	32.012
9	Images	33.012	33.012
10	Smile	32.013	32.013

Table IV (a). The PSNR Value Comparison Table (Image Hiding)

The Image Hiding with the images compared with the PSNR value of input images and output retrieved images. The Fig III represented the comparison of input image and output retrieved image. The Fig IV represented the Text Hiding using the images. The PSNR value compared with the input of the text hiding input and also the retrieved output.

The input and output are compared with the same values means the output and input images are same. The retrieved images compared with the input images. The Peak Signal Noise Ratio can be calculated from the value MSE. The Mean Square Error represented the array of images used in the system.

SI.NO	NAME OF THE IMAGE	PSNR OF INPUT IMAGE	PSNR OF OUTPUT IMAGE
1	Lena	32.967	32.967
2	Gold hill	33.423	33.423
3	Tank	33.784	33.784
4	Monkey	31.606	31.606
5	Nature	32.976	32.976
6	Rail	32.973	32.973
7	Flower	30.523	30.523
8	PC	31.012	31.012
9	Images	33.512	33.512
10	Smile	32.213	32.213

Table IV (b). The PSNR Value Comparison Table (Text Hiding)

SI.NO	NAME OF THE VIDEO	PSNR OF INPUT VIDEO	PSNR OF OUTPUT VIDEO
1	Nature	43.228	43.228
2	Sunrise	40.568	40.568
3	sea	41.956	41.956
4	Hill	43.258	43.258
5	forest	41.986	41.986

Table IV (c). The PSNR Value Comparison Table (Image Hiding)

The Fig V and Fig VI represented the Image Hiding and Text Hiding used with the Video. The Video can be taken as number of frames. One of the frames can be used to embed the data. The Video can be compared with the PSNR values for Image and Text Hiding.

The value are compared with the input and output videos can be used for the RDH process. The Input and Output video can be get the same value. Then the output and input are the same. The retrieved images compared with the input images. The MSE and PSNR values are related in the sense of error rating.

SI.NO	NAME OF THE VIDEO	PSNR OF INPUT VIDEO	PSNR OF OUTPUT VIDEO
1	Nature	42.228	42.228
2	Sunrise	41.568	41.568
3	sea	43.956	43.956
4	Hill	42.558	42.558
5	forest	41.586	41.586

Table IV (d). The PSNR Value Comparison Table (Text Hiding)

The Image and Text Hiding used for Image and Video. The Input and Output values are compared. The analysis concludes the Reversible Data Hiding using Image and Video using Encryption and Decryption with a successful results.

5 CONCLUSION

The Reversible Data Hiding approach used in the proposed method with contrast enhancement using encryption and decryption. The 2 peaks values are selected for hiding the data into the image. The histogram is to be used to surely find out the 2 highest peak values. In the proposed approach is also used for the military and medical areas also. For the sake of histogram specification the image is used. The histogram values analogize to that image pixel value. The proposed approach is used in the color images. For the sake of increasing the enhancement to use the contrast enhancement method. It is more important than storing the PSNR value high. The contrast enhancement put up the light on visual inspection through medical or satellite images and there by fulfilled the desires too. It is a known fact that PSNR value of the enhanced image is less. Image visibility is also been improved. To the best knowledge, there is no existing RDH algorithm that performs the task of contrast enhancement.

For providing high security for the whole system XOR-Encryption and XOR-Decryption techniques used. The Reversible Data Hiding techniques providing with high efficiency and high security. This current techniques works well with both Images and videos.

REFERENCES

[1] Nosrati * Ronak Karimi Mehdi Hariri," Reversible Data Hiding:Principles, Techniques, and Recent Studies". World Applied Programming, Vol (2), Issue (5), May 2012. 349-353ISSN: 2222-2510©2011 WAP journal. www.waprogramming.com

[2] Subhanya R.J (1), Anjani Dayanandh N (2)" Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014)

[3] X. Zhang, "Separable reversible data hiding in encrypted image," IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[4] O. Elbadawy, M. R. El-Sakka, and M. S. Kamel, "An information theoretic image-quality measure", Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, vol. 1, pp. 169-172, 1998.

[5] N. Taneja, B. Raman and I. Gupta, "Combinational domain encryption for still visual data", Journal of Multimedia Tools and Applications, DOI 10.1007/s11042-011-0775-4, (2011).

[6] K. C. Ravishankar and M. G. Venkateshmurthy, "Region Based Selective Image Encryption", International Conference on Computing & Informatics, ICOCI 06, IEEE, Kuala Lumpur, (2006).

[7] I. Ozturk and I. Sogukpınar, "Analysis and Comparison of Image Encryption Algorithms", Journal of transactions on engineering, computing and technology, vol. 3, (2004), pp. 38.

[8] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890– 896, Aug. 2003.

[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354– 362, Mar. 2006.

[10] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.

[11] M.-Z. Gao, Z.-G. Wu, and L. Wang, "Comprehensive evaluation for HE based contrast enhancement techniques," Adv. Intell. Syst. Applicat., vol. 2, pp. 331–338, 2013.

[12] Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast-sensitive reversible visible image watermarking technique," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 5, pp. 656–667, May 2009