Reversible Data Hiding using SST Algorithm

[1]Jagadish M C, [2] C Prabhavathi
[1]M.Tech., Digital Communication Engineering, Siddaganga Institute of Technology Tumkur, India,
[2]Associate Prof. Dept. of Telecommunication Engineering, Siddaganga Institute of Technology Tumkur, India ,
[1]mc.jagadish007@gmail.com,[2]prabhachannaveer@gmail.com

Abstract: **This paper presents the method for reversible data hiding with lossless recovery of the original image. A modified difference expansion algorithm is used in this scheme for reversible data hiding, the algorithm thus increases the amount of data that can be hidden in the image and also guarantees the lossless recovery of the original image. For more security the image is encrypted using the Sieving, Shuffling and Transformation (SST) algorithm.**

***Index Terms*—Difference Expansion, Reversible Data Hiding, SST**

I. INTRODUCTION

The process of embedding useful information into a cover media is called as data hiding. In most of the cases cover media will experience the distortion due to data hiding and cannot retrieve the original image. In medical diagnosis and law enforcement type of applications it is desired to obtain the original image without distortion. The technique which satisfy these requirements is called as reversible data hiding.

Reversible data hiding (RDH) is a technique to embed the additional message in some distortion less cover media. In other data hiding techniques, only the hidden data is recovered at the receiver. In reversible data hiding both the cover image and hidden data are recovered at the receiver. The block diagram of reversible data hiding is shown in Fig.1. The applications of reversible data hiding are authentication, military, law enforcement.

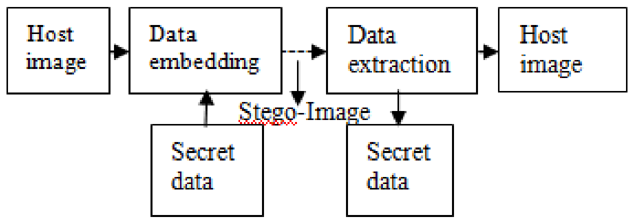


Fig.1. Reversible Data Hiding

There are two basic approaches in RDH [1]:

1. ***Vacating Room After Encryption (VRAE):***

In this method the room for data hiding is done after the encryption of image, it is relatively difficult and inefficient sometimes.

2. ***Reserving Room Before Encryption (RRBE):***

To overcome the limitations of VRAE this method is used. In this method the room is reserved before the encryption for data hiding.

When the data is hidden into the image the image should not be revealed to the unintended user. Thus image can be protected by various types of encryption algorithms. The algorithms are classified into two categories: substitution and transposition. In substitution based encryption it changes the pixel values to make the content unrevealed. In transposition based encryption the pixels are shuffled and no change is made to the pixel values.

The algorithm used is a combination of two methods that are reversible data hiding and visual cryptography. In visual cryptography Sieving Shuffling and Transposition algorithm (SST) algorithm is used[2]. Tian has proposed difference expansion scheme for gray scale images [3]. In this approach it is modified for the color images by reversibly embedding the data for each color components, which increases the capacity of the data to be hidden.

This paper is divided into four main sections. Section II gives details of proposed scheme, section III gives details on algorithms and implementation, section IV is about experimental results and section V is overall conclusion.

II. PROPOSED SCHEME

In this paper, a hybrid algorithm which combines two different approaches that is reversible data hiding and visual cryptography is used. In most of the RDH methods finding the room for data hiding in encrypted images by reserving the room, since vacating room after encryption is difficult and inefficient. In order to avoid this difficulty vacating the room before encryption is to be done. Security of the cover image is also matter of concern after hiding the data. In this scheme, the keys are not used for encryption. It gives low bandwidth and storage requirement, which also decreases the computational cost during encryption and decryption.

The framework for client-server model of the scheme is shown in Fig.2. It involves five main steps; Reserving room for embedding data, Data Embedding in reserved room, Image Encryption using keyless SST algorithm, and Original image reconstruction and Data extraction.

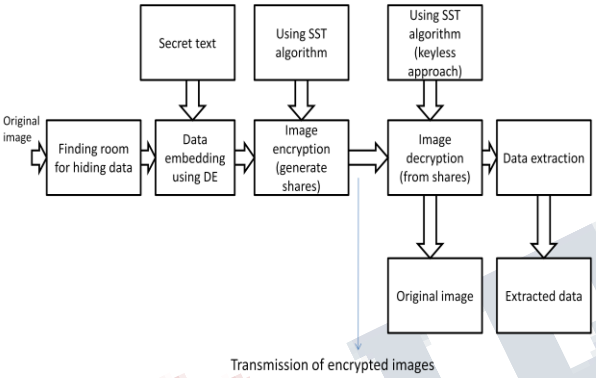

Secret text
Using SST algorithm
Using SST algorithm (keyless approach)
Original image
Finding room for hiding data
Data embedding using DE
Image encryption (generate shares)
Image decryption (from shares)
Data extraction
Original image
Extracted data
Transmission of encrypted images

Fig.2. Framework for client-server model

III. ALGORITHM AND IMPLEMENTATION DETAILS

Steps involved in this scheme are:

- Finding room for data embedding.
- Improve high capacity data embedding using difference expansion.
- Image encryption by dividing the image into shares(based on SST)
- Image decryption.
- Data extraction.

All the steps are implemented using MATLAB.

3.1. Finding Room for Data Hiding.

The common approach for high capacity data embedding is to find the room for embedding data. Finding room for embedding data before encryption is quite efficient, as after encryption the entropy of image changes thus making the process of finding room for embedding data quite difficult. The scheme involves partitioning the image logically into two regions; the goal of image partition is to construct a smoother area B, on which data will be embedded. Let us consider, the original image C is a color image with size M×N and considering separate color component the pixel in each color component matrix will be C(i,j)∈[0,255], 1≤ I ≤ M, 1 ≤ j ≤ N. First, the content owner finds several blocks along the rows from the original image. Several blocks whose number is determined by the size of the embedded messages are denoted by l. Image will be divided into number of blocks with each block consisting of m rows, where m=⌈l/N⌉, and the number of blocks can be computed from No_of_Blocks=⌈M/m⌉. For every block a function is defined to measure its first order smoothness with the help of function *f* [1],

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u+1,v} + C_{u,v+1}}{4} \right| \quad (1)$$

Here, f relates to blocks which contain relatively more complex textures. The content owner then selects the blocks with relatively lower f value as 'B' which is logical smoother area to hide the data as shown in Fig 3. For deciding over the smoother area the average value of f-value of all the blocks is considered and the blocks with f-value below average is considered to be relatively smoother. Only these smooth blocks are considered for hiding data which improves the performance of data hiding process remarkably.

```
if(f-value$_{i\text{-block}}$ < f-valur$_{avg}$)
    then
            block$_{index}$[i]=1
    else
        block$_{index}$[i]=0
```

Thus blocks with index value 1 will be used for data hiding in the data embedding phase. For hiding the data, a reversible data hiding algorithm using difference expansion (DE) will be used in the next step.

DE-based algorithm doesn't take the content of image into account; it brings big distortion to images when the texture of the image is complex. In this scheme, the image is divided logically into smooth and complex regions. Only Smooth region is used for applying RDH and DE algorithm which improves the performance of RDH algorithm. Also the distortion caused to the complex region of image will be less compared to other schemes. Thus visual quality of encoded image is improved by this process.

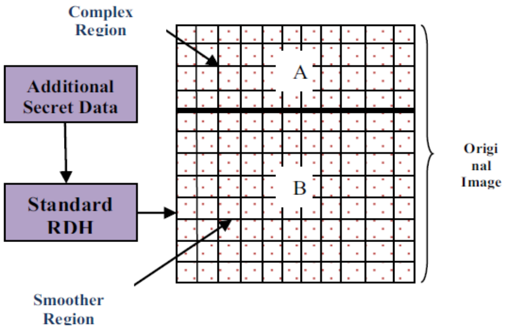


Fig.3.Logical partition of an image

The image is divided into blocks as shown in Fig.3 and the variances of each block are computed to classify the block into different class with different texture. Then different amount of data are embedded into different block, thus improving the quality and increasing the data size.

3.2. Improved High Capacity Data Embedding Using Difference Expansion.

Difference expansion is a high capacity reversible data hiding technique introduced by Tian[3]. This technique is applied for gray scale images, which discovers the extra storage space by exploring the redundancy in the image content. In this paper, the DE method is implemented for color images. The data bits are embedded in each color component as the input image considered is a color image.

3.3. Image Encryption By Dividing Image Into Shares Based on SST Algorithm.

The design of an encryption algorithm will provide extra security to existing reversible data hiding system.

There are three approaches in image encryption.

1. ***Key oriented algorithm:***
   The key based algorithms are very bulky to manage as key handling to be done.
2. ***Image splitting:*** In this technique image is divided into multiple shares, individual shares should not convey any information about the original image, but the proper arrangement of shares will regenerate the image. The limitation of this scheme is pattern will be recognized.
3. ***Multiple shares***: In this without any key the image is encrypted and involves splitting the image into multiple shares.

This encryption scheme is divided into two types:

1. ***Sieving, division and shuffling(SDS) algorithm:***

In sieving process the combined RGB components is divided into individual R, G and B components. In the division process the split images is generated and also divided randomly. In the shuffling process each generated shares are shuffled.

The SDS algorithm has few limitations:

- ❖ Image size is less
- ❖ Pattern will be easily recognized.
- ❖ High computation is involved in encryption.
- ❖ The encryption algorithm is poor in security.

2. ***Sieving, Shuffling and Transformation (SST) algorithm:***

To avoid the above limitations of SDS algorithm and to increase the security level the SST algorithm is used. In this vertical and horizontal shuffling is used to shuffle the image pixel bits and then the transformation technique is used to convert the image into unreadable image format. The overall architecture of the SST algorithm is shown in Fig. 4[4].

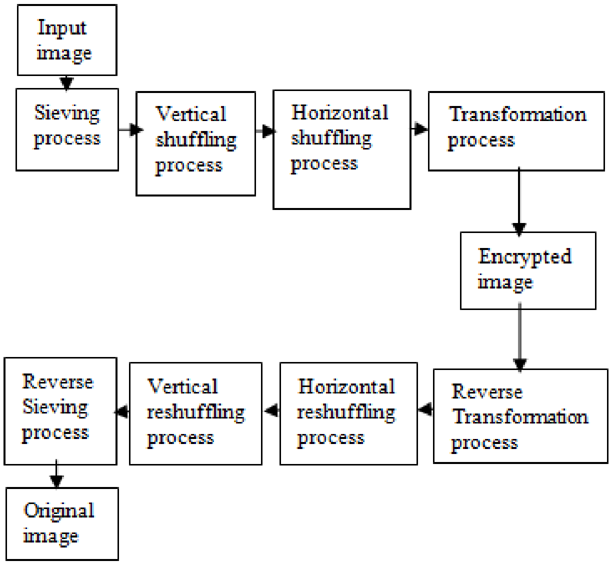

Input image
Sieving process
Vertical shuffling process
Horizontal shuffling process
Transformation process
Encrypted image
Reverse Transformation process
Horizontal reshuffling process
Vertical reshuffling process
Reverse Sieving process
Original image

Fig.4. Architecture of SST algorithm

Sieving: Sieving process involves filtering the combined RGB components into individual R, G and B components.
Shuffling: It performs the shuffle operation of sieving image. Shuffling technique has 2 phases to shuffle the pixel bits in original image. Here, vertical and horizontal pixel bits swap to adjacent pixel bits value in vertical and horizontal manner.
Transformation: This process transforms the horizontal image into unreadable image format.

3.4. Image reconstruction by combining received shares and data retrieval at client side.

Image reconstruction by combining received shares and data retrieval at client side as shown in Fig.5 is the reverse process that is performed in the encryption process SST. The retrieved image is as same as the original image and there is no loss of picture quality in the reconstructed image.

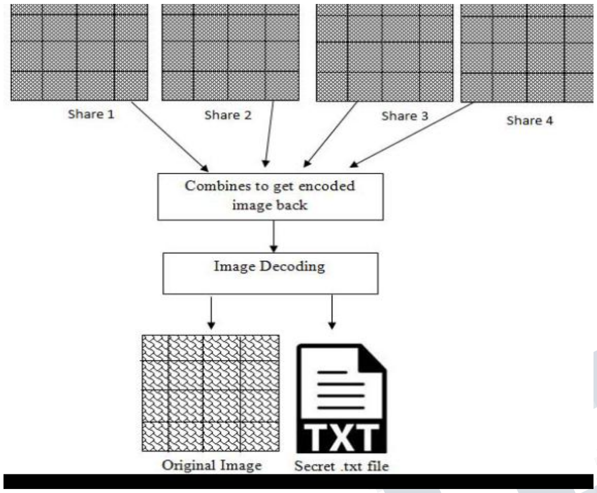


Fig.5. Image reconstruction by combining received shares and data retrieval at client side.

IV. EXPERIMENTAL RESULTS

The proposed algorithm is implemented using MATLAB. All computations are performed by embedding and decoding actual bit stream in the form of .txt file. The results are evaluated with the help of standard PSNR value.

$$\text{PSNR} = 10 \times \log_{10}\frac{MAX_f}{MSE} \text{ - - - (2)}$$

Formula for MSE (Mean Square Error) is given as:

$$\text{MSE}=\frac{1}{m\ x\ n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(f_{ij}-g_{ij})^2\text{- - - (3)}$$

Where, g is matrix data
M is number of rows of pixel
N is number of column of pixel
MAX_f is maximum signal value

This method is applied on various standard color images of various sizes. The operation at the server side is shown in Fig.6. First the input image file and text file is selected. Here size of flower.jpg image is 256x256 and size of message.txt data file is 20680. After selecting hide data button the text file gets successfully hidden in the image file. The PSNR value of original and encoded image is calculated for analysis purpose. Data to be hidden in the image is shown in Fig.7 and watermarked image which contains the data is shown in Fig.8.

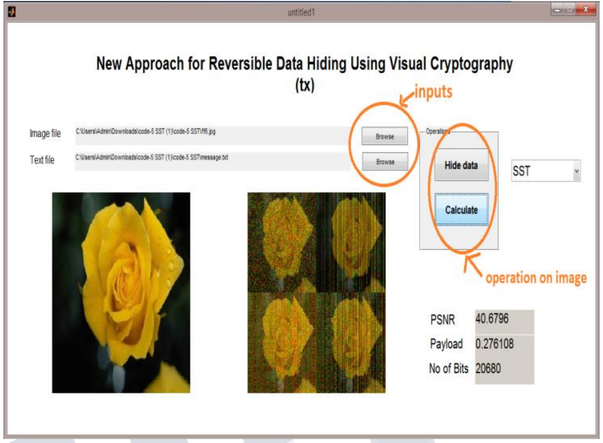
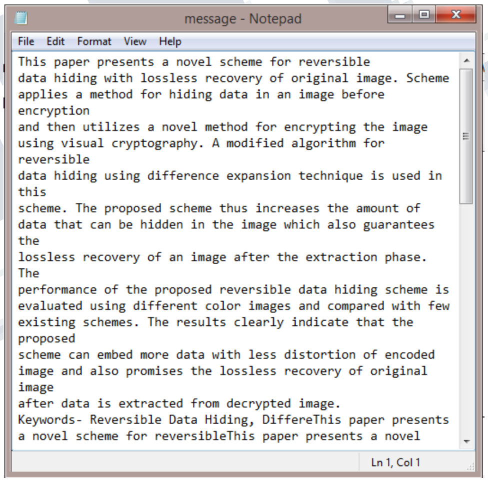


Image file C:\Users\Admin\Downloads\code-5 SST (1)\code-5 SST\ff6.jpg
Text file C:\Users\Admin\Downloads\code-5 SST (1)\code-5 SST\message.txt
SST
PSNR 40.6796
Payload 0.276108
No of Bits 20680

Fig.6. Operation at the server side



```
This paper presents a novel scheme for reversible
data hiding with lossless recovery of original image. Scheme
applies a method for hiding data in an image before
encryption
and then utilizes a novel method for encrypting the image
using visual cryptography. A modified algorithm for
reversible
data hiding using difference expansion technique is used in
this
scheme. The proposed scheme thus increases the amount of
data that can be hidden in the image which also guarantees
the
lossless recovery of an image after the extraction phase.
The
performance of the proposed reversible data hiding scheme is
evaluated using different color images and compared with few
existing schemes. The results clearly indicate that the
proposed
scheme can embed more data with less distortion of encoded
image and also promises the lossless recovery of original
image
after data is extracted from decrypted image.
Keywords- Reversible Data Hiding, DiffereThis paper presents
a novel scheme for reversibleThis paper presents a novel
```

Fig.7. Data to be hidden

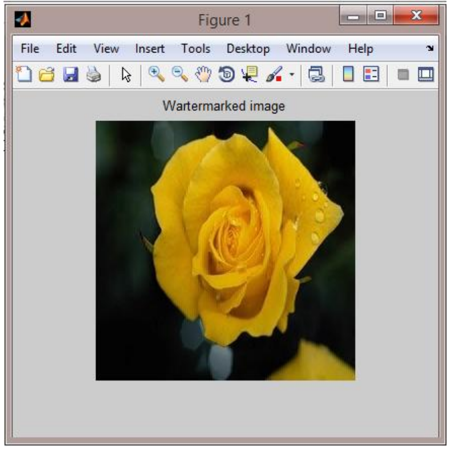
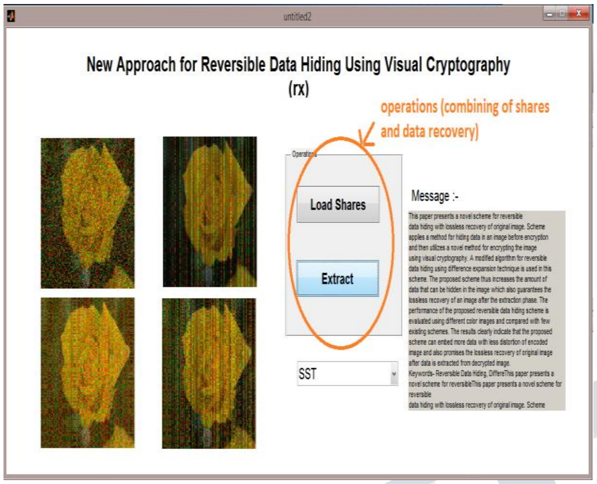


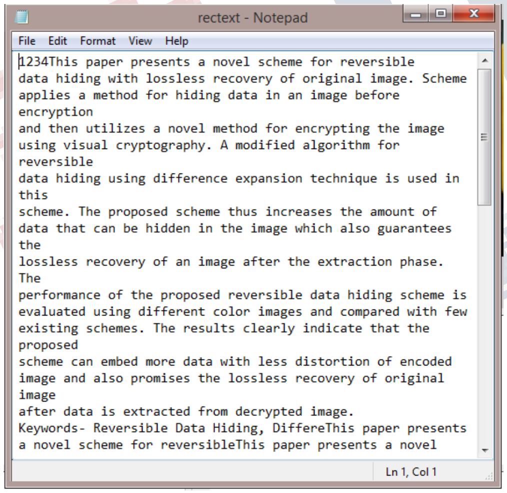
Fig.8. Encoded image

The operation at the receiver side is shown in Fig.9. First the shares that are generated at the transmitter side which is sent through LAN are loaded by clicking the load share button and then the original image and data is obtained by clicking the extract button. Data extraction from the share is shown in Fig.10. The reconstructed image is shown in Fig.11. The recovered image and the text file are same as the original.


untitled2
New Approach for Reversible Data Hiding Using Visual Cryptography
(rx)
operations (combining of shares
and data recovery)
Operations
Load Shares
Extract
SST
Message :-

```
This paper presents a novel scheme for reversible
data hiding with lossless recovery of original image. Scheme
applies a method for hiding data in an image before encryption
and then utilizes a novel method for encrypting the image
using visual cryptography. A modified algorithm for reversible
data hiding using difference expansion technique is used in this
scheme. The proposed scheme thus increases the amount of
data that can be hidden in the image which also guarantees the
lossless recovery of an image after the extraction phase. The
performance of the proposed reversible data hiding scheme is
evaluated using different color images and compared with few
existing schemes. The results clearly indicate that the proposed
scheme can embed more data with less distortion of encoded
image and also promises the lossless recovery of original image
after data is extracted from decrypted image.
Keywords- Reversible Data Hiding, DiffereThis paper presents a
novel scheme for reversibleThis paper presents a novel scheme for
reversible
data hiding with lossless recovery of original image. Scheme
```

Fig.9. Operation at the receiver side



```
1234This paper presents a novel scheme for reversible
data hiding with lossless recovery of original image. Scheme
applies a method for hiding data in an image before
encryption
and then utilizes a novel method for encrypting the image
using visual cryptography. A modified algorithm for
reversible
data hiding using difference expansion technique is used in
this
scheme. The proposed scheme thus increases the amount of
data that can be hidden in the image which also guarantees
the
lossless recovery of an image after the extraction phase.
The
performance of the proposed reversible data hiding scheme is
evaluated using different color images and compared with few
existing schemes. The results clearly indicate that the
proposed
scheme can embed more data with less distortion of encoded
image and also promises the lossless recovery of original
image
after data is extracted from decrypted image.
Keywords- Reversible Data Hiding, DiffereThis paper presents
a novel scheme for reversibleThis paper presents a novel
```

Fig.10. Data extracted from the shares.

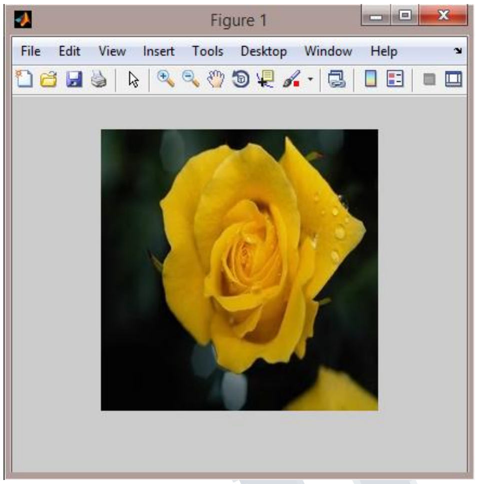


Fig.11. Reconstructed image

Analysis of data hiding algorithm:

As the scheme makes use of improved reversible data hiding scheme using DE, to evaluate its performance various computations are performed on different size. Table 1 shows Embedding Rate and PSNR offered by various color images.

Table 1: embedding rate vs. Psnr comparison of various color images

Embedding capacity (bits)	Embedding rate (bpp)	PSNR Results			
		Flower .jpg	Vegetable.jpg	Ship .jpg	Ring .jpg
20680	0.276108	40.6796	40.357	39.7316	37.9484
14968	0.19984	40.8335	40.5531	39.7317	38.1915
9440	0.126038	41.049	40.7651	39.7855	38.3776

V. CONCLUSION

The scheme which is implemented uses the Reserving Room Before Encryption (RRBE) approach for finding the room for data hiding, and then for hiding data improved Difference Expansion (DE) algorithm is used, which increases the data hiding capacity by hiding data in separate color components. Sieving, Shuffling and Transformation (SST) algorithm is used to encrypt the image after hiding the data at the transmitter side. At the receiver side all the shares are combined to recover the data and original image. This scheme guarantees the lossless recovery of the image and the data.

REFERENCES

[1] Kede Ma. Weiming Zhang, Xianfeng Zhao, NenghaiYu,Fenghua Li, “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, IEEE Trans on Information Forensics and security, Vol. 8, No.

[2] Pratibha S. Ghode, “A Keyless approach to Lossless Image Encryption”, International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 5, May 2014.

[3] Jun Tian, “*Reversible Data Embedding Using a difference Expansion”, IEEE Transaction on circuits and systems for video* technology, Vol.13, No. 8, Aug 2003.

[4]Wei Qiao, HongdongHuaqing Liang, “A kind of Visual Cryptography Scheme For color Images based on halftone technique”, International Conference on Measuring Technology and Mechatronics automation © 2009 IEEE.

[5]Siddharth Malik, Anjali Sardana, Jaya, “A Keyless Approach to Image Encryption”,2012 international conference on Communication systems and Network Technologies ©2012 IEEE.

[6]A.M Alattar. ”Reversible watermark using the difference expansion of a generalized integer transform”. IEEE Trans. Image process. 2004Vol. 13, No. 8, pp. 1147-1156