ISSN No. 0976-5697

Volume 7, No. 5, September-October 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Image Interpolation Based Reversible Data Hiding Scheme Based on Pixel Intensity

Sonika Payal
Department of Computer Science & Engineering
Shekhawati Engineering College, Dundlod, Jhunjhunu
Rajasthan, India

Gyanchand Yadav
Department of Computer Science & Engineering
Shekhawati Engineering College, Dundlod, Jhunjhunu
Rajasthan, India

Abstract: In this paper, we propose two interpolations based reversible data hiding scheme. In the first scheme, we propose a novel reversible stenographic scheme using image interpolation and pixel intensity. The scheme consists of two stages namely: image interpolation and data hiding. At the first stage i.e., image interpolation, the original image is scaled up using the INP (Interpolation by Neighboring Pixels) and then at the second stage i.e., data hiding, the secret data is hidden into the interpolated pixels. The amount of secret data is hidden into the pixels based on the intensity of the pixels. The scheme makes use of a notion that more changes can be tolerated in high intensity pixels than in the low intensity ones. Finally, we compare our scheme with some of the important schemes of the literature. The experimental results show that our schemes perform better in terms of hiding capacity and image quality.In the second scheme, we propose a reversible data hiding scheme using image interpolation which embeds the secret data bits into two passes after scaling up the input image using the INP (Interpolation by Neighboring Pixels). Only interpolated pixels are used to embed the secret data. In the first pass, it embeds the secret data into the even valued pixels followed by second pass in which odd valued pixels are used to embed the secret data. Before embedding the secret data in every pass, it constructs a location map which is compressed using JBIG1 compression technique and is sent to the receiver using a secure channel. To improve the security of the secret message, it selects a private key and XORes all the bytes of the secret data before embedding the same into the image so that even if the attacker cracks the embedding algorithm he/she is not able to get the original; secret data. Experimentally, our scheme performs much better than the existing scheme in terms of both data hiding capacity and image quality. Furthermore, it is very simple as it only increases or decreases the pixel values for embedding the secret data.

Keywords: cover image, stego image, reversible data hiding, interpolation, secret data, hiding capacity, image quality.

I. Introduction

Today, communication can be done between two or more persons being at different places through internet. For confidential communication, i.e., the communicating message is not revealed, the message must be encrypted before sending. If the confidential message (i.e. encrypted) is detected by an attacker, it may be vulnerable. The solution for such types of problems is provided by steganography. The word 'steganography' is the combination of two Greek words - *stegano* and *graphy* which mean *covered* and *writing* respectively in English. In fact, there are three major branches of information hiding namely **DigitalWatermarking**, **Cryptography** and**Steganography** [1].

In **Digital Watermarking,** a secret message is embedded in the given digital signal for the purpose of verifying the authenticity or the identity of the owner of that signal. It is similar to a paper bearing a watermark for visible identification. Watermark can be visible or invisible depending on the application. The visible watermark is generally used for authorization purpose, whereas invisible watermark is used to check the originality of the signal or data. In **Cryptography,** the secret data/ message is encrypted by using a key and the resultant message is called cipher text/message. There are two main classes of cryptography: Symmetric and Asymmetric cryptography. In Symmetric cryptography, a key is used that is known to both sender and receiver, whereas in asymmetric cryptography there are multiple keys some of them are known either to the sender or the receiver.

Steganography is mainly used for hiding the secret data in such a way that the existence of the secret message cannot be detected. In a Steganography technique, the secret data is embedded into a given media, called cover media, in such a way that the existence of secret data cannot be sensed. The basic model of steganography uses the cover media in which secret data is embedded, secret data that is to be hidden, and the algorithm with secret key through which secret data is embedded into the cover media and can be extracted, if required. The cover media or secret data/ message can be textual data, audio data or video data. A steganography technique produces the stego media (the media that has the secret message) from the cover media and secret data [2]. In present work, we use image data as a cover media and secret data as random bit stream.

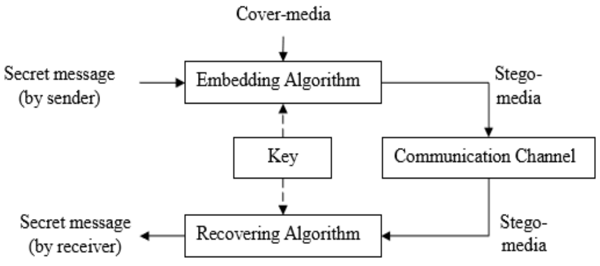


Fig. 1: Basic Steganography Model

Digital data is easy to copy and delete/modify by an illegitimate person while in transmission. Therefore, a need to transfer data securely is emerged. Data hiding is the art of hiding message within another so that presence of hidden message is indistinguishable. The key concept behind data hiding is that message to be transmitted is not detectable to the casual eyes [3].

Any data hiding system can be comprehended as shown in Fig. 1. For a steganographic algorithm having a stego-key, given any cover image the embedding process generates a stego image. The extraction process takes the stego image and using the shared key applies the inverse algorithm to extract the hidden message.

A data hiding method has three main characteristics: capacity, security, and robustness [4-7].

- The capacity refers to the amount of data in terms of bits hidden in the cover medium.
- The security is related to the ability of an eavesdropper to figure out the hidden information.
- Robustness is concerned about the resistance of modifying or destroying unseen data [2].

Requirements for higher capacity and secure communication are often contradictory. However, depending on the specific application scenarios, a tradeoff has to be sought.

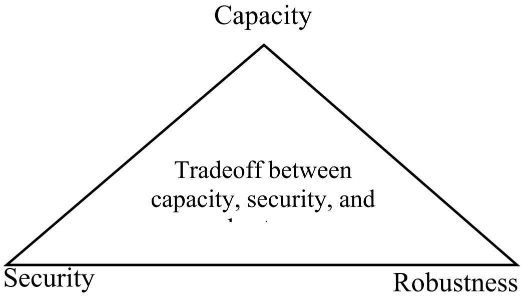


Fig 2: Tradeoff in data hiding between embedding capacity, security, and robustness.

Usually, data hiding techniques are divided into two categories: reversible and irreversible data hiding techniques based on what happens to the original image after recovering the data from the stego-media. In reversible data hiding techniques, the original cover image can be recovered after extraction of the secret data while in irreversible data hiding it is not possible. The cover media to hide the secret data can be images, text, video etc. The image data hiding methods use image as cover media. In some applications, such as medical diagnosis and law enforcement, it is mandatory to reverse the stego-media back into the original cover media after the extraction of the hidden message for some legal considerations. In other applications, such as remote sensing and high energy physical experiment investigation, it is also desired that the original cover media can be recovered because of the required high precision nature. The data hiding techniques which satisfy the requirement are referred to as reversible data hiding techniques [12].

Data hiding can be divided into three domains based on the different image properties: spatial domain [7-12], frequency domain [13-14], and compression domain [15-16]. The spatial domain based techniques hides the secret data directly into the pixel values. The very popular and simple data hiding technique is LSB substitution [17] in which the LSB of the pixels are replaced by the bits of the secret data. In Least significant bit (LSB) insertion method,the secret data bits are embedded into the LSB of the pixels. The least significant bit insertion method is the most obvious but the most commonly known approach for hiding the secret information in a cover image. The number of LSBs into which the secret data bits are embedded may be fixed or variable. In case of fixed LSBs, same numbers of LSBs are used. This method is quite simple but increasing the size of secret data distorts the stego image. In this method, every pixel value is modified in equal amount without analyzing the human observation. In case of variable LSBs, the number of LSBs are determined according to some characteristics of the pixel e.g., intensity value of the pixel or intensity of the neighboring pixels. Almost all the LSB based techniques use variable number of LSBs for embedding the secret message. Some of the methods identify pixels which are optimal in a sense besides the desired number of LSBs which enhances the security of the secret data as well as increases the hiding capacity without losing much image quality. If the stego image is altered or compressed with some lossy compression technique, the extraction of secret data may not be possible. Another scheme to embed the secret data using the spatial domain is histogram modification method which shifts the pixels values for embedding the secret data. This scheme can hide sufficient data with good image quality. There have been many improvements in the histogram based data hiding schemes so that more secret data can be hiding with better image quality. [21-23]. Image interpolation [24-30] is generally another spatial domain based data hiding technique to embed the secret data generating a high-resolution image from its low-resolution. The secret data is hidden into the interpolated pixels which may have slightly different values than the original pixels so that a good quality stego-image is provided with high data hiding capacity. There are some simple interpolation methods, such as nearest neighbor, bilinear, and nearest neighbor mean interpolation etc. The frequency domain based data hiding techniques first of all transforms the cover image into frequency coefficients and then hides the secret data into the coefficients. Some wellknown transformation functions such as discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT) and so on are usually employed. In the compression domain, the cover image is firstly compressed and then the secret data is embedded into the compressed codes. In our work, we scales up the image using Interpolation by neighboring pixel method and then hide the secret message into the scaled pixels. Our methods perform better than R weighted coding method and many other approaches in terms of PSNR value and capacity of hiding secret data.

Rest of the paper is organized as follows. Section II discusses the literature survey. A new image interpolation based reversible data hiding scheme using pixel intensity is discusses in section III with the results and discussion. Section IV discusses a second image interpolation based reversible data hiding scheme using complementary embedding with the results and discussion section. Finally, paper is concluded in section V.

II. LITERATURE SURVEY

The term steganography is existed since 440 B.C. A good amount of work has been done since its origination, but the major advancements in terms of quality have been done in last 15-20 years. The probable reason is that image processing applications require large amount of resources including computing power, storage requirements which were not supported by the then systems. Now, working on the images or videos has become efficient and effective because of the major improvement in the computer and communication technologies. The today's even low end systems can process easily the images/ videos in any domain that is transform domain or spatial domain. These approaches used in these areas make use of the characteristics of digital image in hiding the secret data. The various important techniques that are based on transform and spatial domain are discussed below:

This LSB substitution method [32] can hide a message of any form, be it image, text, audio, etc. and its capacity is of significant size. It can recover the hidden data and also maintain the size of original image. Another important method based on optimal LSB Substitution and Randomization is given by Wang et al. [32, 33]. This method hides secret message in the cover image in such a way that the existence of message cannot be noticed by human eyes. Thus it increases the security and efficiency of the system. The optimal LSB Substitution is effective even in worst case. However, when data is to be hidden in large number of LSBs of the cover image, it requires large computation for embedding and also for extraction. The optimal solution in such case is obtained using genetic algorithm. In these schemes, no characteristics of human visual system have been explored. Wu et al. [34] discuss an important method that exploits characteristics of human visual system and makes use of Least Significant Bit (LSB) replacement and Pixel Value Differencing (PVD). In this method, the image is divided into number of non-overlapping blocks and then difference value is calculated between two consecutive pixels for each block. The difference values range will be in -255 to 255. Hence, the block with large value is considered as an edge area and for small value, it considered as smooth area because the human eyes are more sensitive to edge areas compared to smooth area. The small or large values are taken based on some pre-specified threshold value. This method embeds more bits in edge areas in contrast to smooth areas. Here, the main focus was on increasing the capacity of data to be embedded. H.B. Kekre [35] discussed a method which was presented as an improvement in PVD technique. Here first of all a secret key of 8 bits is selected then XOR operation is done between the same key and all bytes of secret message. Now we analyze each pixel of cover image and embed the resultant secret message. If the embedding pixel intensity of the cover image is greater than 239 and bit to be embedded is 1 we embed 5 bits of secret text otherwise (the bit to be embedded is 0), 4 bits are embedded in the LSBs of that pixel and if pixel intensity is in the range of 224 to 239 and bit to be embedded is 0 then we embed 5 bits of secret message otherwise (the bit to be embedded is 1), 3 bits are embedded and if the intensity is in the range of 192 to 223 then we embed 2 bits otherwise only one bit is embedded in LSB of that pixel. Here matrix entries are also maintained if data to be embedded in single pixel is 5 bits. Hence capacity of the image is increased if the image is of high intensity pixels otherwise capacity can remain low.

Image interpolation [24, 25] is simply used to generate a high-resolution image from its low resolution, that is, to scale-up an image. The interpolated pixel result to some difference values comparing with its original image and data hiding can be applied by taking this advantage. There are some simple interpolation methods, such as B-spline, cubic, bilinear, bi-cubic, Lagranges and Guassian which have been used in re-sampling [24]. Image interpolation methods are as old as computer graphics and demands for image processing. Simple interpolation methods like NMI or nearest neighbor, B-spline, cubic, bilinear, bi-cubic, Lagranges and Guassian have been used re-sampling [24]. The nearest neighbor method finds the closest corresponding pixels of the cover image for each block and set them to a new pixel value for the destination image using neighboring pixels. The bilinear method determines the new value from the weighted average of the four closest pixels. Recently, the interpolation by neighboring pixel is discussed in [24]. This method increases the payload in data hiding. An important method which uses interpolated images to hide the secret data in order to increase the hiding capacity and improve the visual quality is the R-weighted coding method (RCM) [27]. This method is only applicable to hide secret data into the RGB color images. Hence a need of hiding secret data into gray as well as in RGB color images efficiently and effectively arises. Jung and Yoo [25] discussed a data hiding method using interpolation. This method firstly scales down an input image to quarter of its initial size and then an interpolation is used to scale up the image to produce a cover image of initial size before embedding occurs. The secret message is then embedded into the cover image to produce a stego-image. The number of secret data bits to be embedded is the log values of the differences of the pixels. On the receiving side, the secret message can be extracted from the stego-image and the original image is recovered. This method can hide the secret data into both gray and color images. Another important method discussed by Chang et al [30] is based on interpolation in conjunction with pixel shifting histogram. This method modifies the interpolation method to hide the more secret data and also enhance the quality of the resultant interpolated image. In embedding phase, the pixel shifting histogram method is used to hide the secret data. In our proposed method, we try to hide more secret data while preserving the image quality. We make use of pixel intensity to hide the secret data, hence, we don't need the characteristics of color images means both gray and RGB images can be used to hide the secret data.

The methods discussed above have trade off capacity versus quality. In other words, if the number of bits of the secret data is low, the stego image quality is high and vice versa. In our work, we embed less number of bits in the pixels having low intensity pixels and more bits in the higher intensity ones. By doing this the data hiding capacity is increased without degrading the quality of the stego image.

III. IMAGE INTERPOLATION BASED REVERSIBLE DATA HIDING SCHEME USING PIXEL INTENSITY

In previous section we have discussed newly developed important data hiding schemes. All these method have a trade off between image qualities with data hiding capacity. That is if the amount of secret data is increased, the image quality degrades and vice versa. In our work, we discuss a novel image interpolation based reversible data hiding schemes based on the pixel intensity. The scheme consists of two parts: image interpolation and data hiding. For interpolating the image, Neighbouring pixel Interpolation (INP) method is used. The embedding of secret data is done on the basis of the pixel intensity of the interpolated pixel.

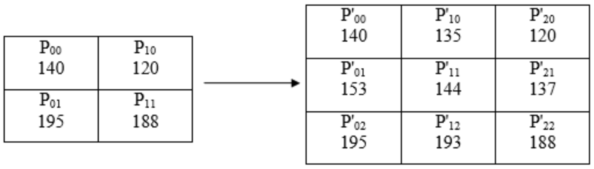
The proposed algorithm consists two phases: embedding phase and extraction phase as given below.

A. *Embedding phase*

The secret data is concealed in the cover image in the embedding phase which is divided into two phases: image interpolation and data hiding. In the image interpolation sub-phase, the cover image is scaled up using Neighbouring pixel Interpolation and then in the data hiding phase the secret data bits are embedded into the scaled pixels based on the pixel intensity values.

1) Neighboring pixel Interpolation

The concept of Neighbouring pixel Interpolation (INP) is that pixels at near neighboring locations tend to have similar intensity values. This means that the image quality can be improved with less distortion. Suppose that a cover image has four pixels. We can calculate the new pixels for up scaling the image 2 times as shown in Fig. 1. So, before scaling up the image, divide the image into 2 by 2 blocks and apply INP method to scale up each block and combine the scaled blocks to get the resultant interpolated image.



P_{00} 140	P_{10} 120
P_{01} 195	P_{11} 188

P'_{00} 140	P'_{10} 135	P'_{20} 120
P'_{01} 153	P'_{11} 144	P'_{21} 137
P'_{02} 195	P'_{12} 193	P'_{22} 188

Fig 3. An example of scaling up process on the INP method

Let P_{00}, P_{10}, P_{01} and P_{11} are the pixel values of cover images

- Calculate P'_{10} as $(P_{00}+ (P_{00}+P_{10})/2)/2$
- Calculate P'_{01} as $(P_{00}+ (P_{00}+P_{01})/2)/2$
- Calculate P'_{11} as $(P'_{10}+ P'_{01})/2)$
- Calculate P'_{21} as $(P_{10}+ (P_{10}+P_{11})/2)/2$
- Calculate P'_{12} as $(P_{01}+ (P_{01}+P_{11})/2)/2$

The interpolated pixels P'_{10}, P'_{01}, P'_{11}, P'_{21}, and P'_{12} are calculated using above formulas and their location in the image is shown in Fig. 3.

2) *Data Hiding*

The secret data will be hidden only in interpolated pixels so that the original image is recovered at the receiver side. Hence, the proposed method is reversible data hiding method. The following algorithm will hide the secret data into the cover image.

Step 1. Select a secret key of 8 bits and XOR with all bytes of secret message.

Step2. Scan the cover image in raster scan manner.

Step3. Embed the secret data into interpolated pixels as follows.

- If pixel intensity of the cover image is in the range of 192 to 255 or 0 to 15 then replace 4 LSBs of the pixel with the 4 bits of the secret data.
- If pixel intensity of the cover image is in the range of 32 to 191 and then replace 2 LSBs of the pixel with the 2 bits of the secret data.
- Otherwise pixel intensity of the cover image will be in the range of 16 to 31 then replace 3 LSBs of the pixel with the 3 bits of the secret data.

Step4. Repeat the step 3 for each interpolated pixel. Thus, a stego image having the hidden secret data is obtained.

The obtained stego-image is transmitted to the receiver.

B. Data Extraction Phase

The extraction phase is performed by the receiver. Here, the receiver reverses the embedding phase to extract the secret data and to recover the original image. After extraction of the secret data, 8 bit secret key with XOR operations is applied on the extracted message to regenerate original message. By removing every interpolated pixel or the pixels which had secret data, the receiver can easily get the original image. The complete algorithm is given as follows:

Step 1. Scan the stego-image in raster scan manner.

Step 2. Extract the secret data from the interpolated pixels as follows:

- If pixel intensity of the stego- image is in the range of 192 to 255 or 0 to 15 then extract 4 LSBs of the pixel into the secret data stream.
- If pixel intensity of the stego- image is in the range of 32 to 191 then extract 2 LSBs of the pixel into the secret data stream.
- Otherwise pixel intensity of the stego- image is in the range of 16 to 31 then extract 3 LSBs of the pixel into the secret data stream.

Step 3. Get the secret i.e. 8 bits key and XOR this with all the bytes of the extracted secret message.

Step 4. Discard the interpolated pixels to get the original cover image.

Thus proceeding, we get the complete hidden secret data and the original image at the receiver side.

C. Experimental Results and Discussions

In this section, we carry out experiments by taking most widely used images for evaluating their performances.In this section, we calculate these parameters for our proposed scheme and compare them with that of the very important reversible data hiding scheme [25, 30]. We have taken nine images as the cover media for covering the variance in the image characteristics.

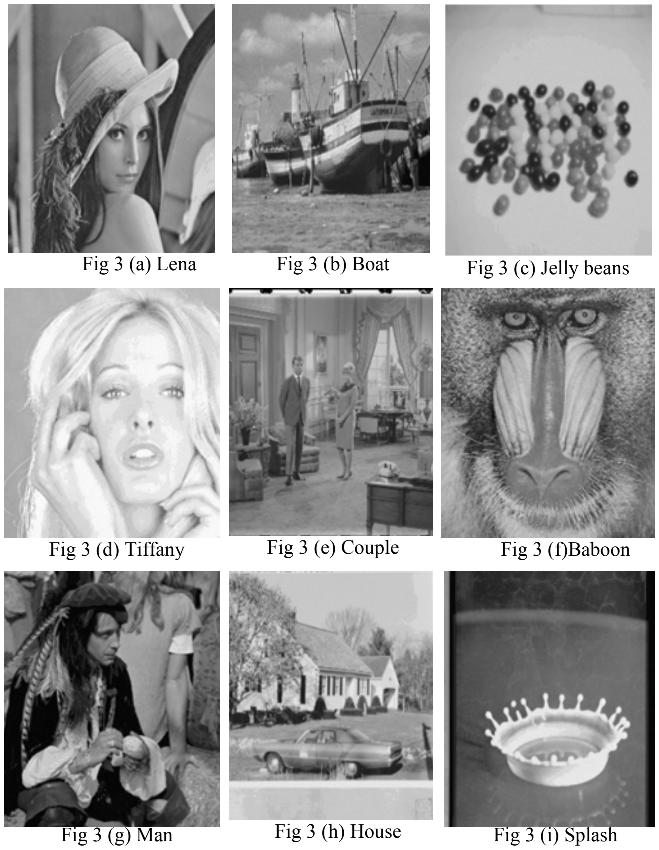


Fig 3 (a) Lena

Fig 3 (b) Boat

Fig 3 (c) Jelly beans

Fig 3 (d) Tiffany

Fig 3 (e) Couple

Fig 3 (f)Baboon

Fig 3 (g) Man

Fig 3 (h) House

Fig 3 (i) Splash

Fig. 3 (a-i) Cover- images, each of size 512x512.

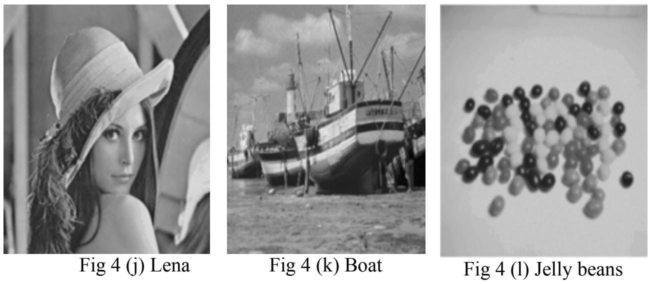


Fig 4 (j) Lena

Fig 4 (k) Boat

Fig 4 (l) Jelly beans

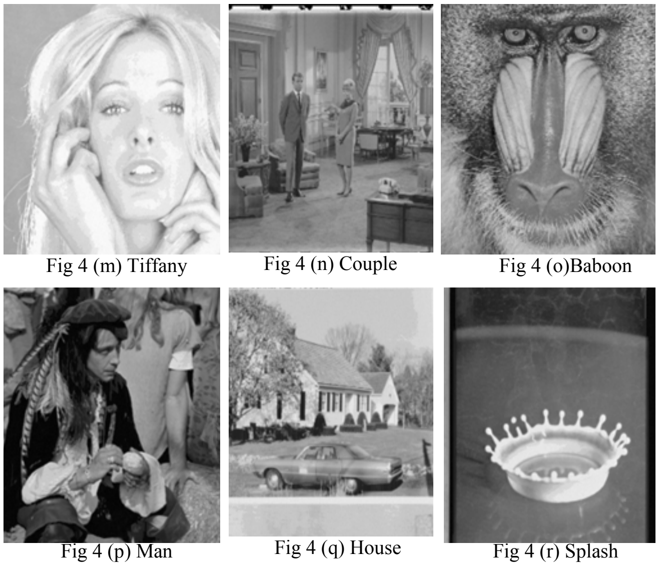


Fig 4 (m) Tiffany Fig 4 (n) Couple Fig 4 (o)Baboon

Fig 4 (p) Man Fig 4 (q) House Fig 4 (r) Splash

Fig. 4 (j-r) Stego- images, each of size 512x512.

The images each of size 512×512 pixels are shown in Figs. 3 (a)-(i). We have implemented the proposed scheme in MATLAB running on the Intel® Core 2 Duo 2.20 GHz CPU, and 3GB RAM hardware platform. The secret data to be embedded is generated using random function.The proposed scheme increases the embedding capacity as it embeds more bits of the secret data into high intensity pixels and also efficiently utilizes the low intensity pixels so that the goal of high capacity and high PSNR is achieved. The results based on the PSNR values and hiding capacities in bits for different data hiding techniques are illustrated in Table 1 &2.

Table 1: A comparison of Jung &Yoo's scheme on capacity with the proposed scheme

Images	Jung and Yoo's method [25]	Chang's method [30] (A)	Proposed method (B)	Percentage increment ((B-A)/A)
Lena	235460	247095	429383	73.77
Boat	226159	269431	421857	56.57
Jelly beans	236545	256974	538474	109.54
Tiffany	202238	227822	443689	94.75
Couple	268389	258555	410554	58.78
Baboon	460740	396651	408251	2.92
Man	256987	278954	476096	70.67
House	246595	259635	541357	108.50
Splash	236595	256935	449366	74.89

Table 2: A comparison of Jung &Yoo's scheme on PSNR with the proposed scheme

Images	Jung and Yoo's method [25]	Chang's Method [30] (A)	Proposed method (B)	Percentage increment ((B-A)/A)
Lena	30.61	43.61	44.2506	1.46
Boat	28.62	41.12	41.4929	0.90
Jelly beans	31.56	36.56	37.6059	2.86
Tiffany	30.23	33.96	37.5062	10.44
Couple	30.88	40.23	45.2007	12.35
Baboon	23.13	34.63	44.6583	28.95
Man	29.36	36.89	39.0137	5.75
House	30.59	35.63	38.7792	8.83
Splash	31.89	38.93	42.6331	9.51

From the Table 1 & 2, it is evident that the proposed scheme is far better than the existing schemes in terms of both the data hiding capacity and visual quality. In fact, it gains the increment in the PSNR value in the range of 0.90 to 28.95% and in the data hiding capacity in the range of 2.92 to 109.54% with respect to Chang et al. method [30]. We have calculated the increment percent with respect to Chang et al. method [30] because its performance is better than the Jung &Yoo method [25] in terms of both the data hiding capacity and image quality. Our scheme provides better quality stego-image because the proposed hiding scheme considers the human visual system into account and then embeds the secret data. It basically makes lesser changes into the pixels having low intensity value and more changes into the pixels of high intensity value. It is because a bigger change made to low intensity pixels might change its intensity value significantly which in turn will rise suspicion however the same amount of change in the high intensity pixel will not have same impact. Thus, our scheme is able to provide a good quality stego-image with high data hiding capacity. The stego-image are shown in Fig. 4 (j-r).

IV. IMAGE INTERPOLATION BASED REVERSIBLE DATA HIDING SCHEME USING COMPLEMENTARY EMBEDDING

In previous work, we have introduced a novel data hiding scheme using image interpolation and pixel intensity which has two phases: image interpolation and data hiding. In this paper, we propose a reversible data hiding scheme which also works in two phases: image interpolation and data hiding. The first phase of this scheme is same as the previous one. However, the second phase namely data hiding phase works differently. Here, it embeds the secret data into two passes. In the first pass, it firstly constructs a location map in which even valued pixels are represented by '0' and odd valued by '1', and then embeds the secret data into the even valued pixels by either increasing their value by one or by leaving them unchanged according to the secret data bit. In the second pass, it again constructs a location map in which even valued pixels are represented by '0' and odd valued by '1', and then embeds the secret data into the odd valued pixels by either decreasing their value by one or by leaving them unchanged according to the secret data bit. The obtained location maps are then combined, compressed using JBIG1 compression scheme, and transmitted through a secure channel. Before embedding the secret data into the image, it XORes each byte of the same with a selected secret key so that security of the secret data is further improved.

In the next subsection, the proposed data hiding algorithm is discussed in a detailed step by step manner.

A. *Data Hiding Phase*

This embedding algorithm embeds the secret data only in interpolated pixels so that the original image is recovered at the receiver side. Hence, the proposed method is reversible data hiding method. The following algorithm will hide the secret data into the cover image.

1) Embedding algorithm

Step 1. Select a secret key of 8 bits and XOR with all bytes of secret message.

Step 2. Scan the cover image in raster scan order and construct a location map (LM1) in which even valued pixels are represented by '0' bit and odd valued by '1' bit.

Step 3. Embed the secret data in each even valued pixel as follows: If the secret data bit is '0'; then increase the pixel value by one, otherwise leave it unchanged.

Step4: Scan the resultant image in raster scan order and construct a location map (LM2) in which even valued pixels are represented by '0' bit and odd valued by '1' bit.

Step 5. Embed the secret data in each odd valued pixels as follows: If the secret data bit is '0'; then decrease the pixel value by one, otherwise leave it unchanged.

Step6: Concatenate the location maps LM1 and LM2 as LM1||LM2 and compress the LM using JBIG1.

Step7: Thus, the resultant image which is a stego-image is obtained.

The compressed location map is transmitted through a secure channel.

2) Data Extraction Phase

The extraction phase is performed by the receiver. Here, the receiver reverses the embedding phase to extract the secret data and to recover the original image. At the end, 8 bit secret key with XOR operations is applied on the extracted message to regenerate original message. By removing every interpolated pixel or the pixels which had secret data, the receiver can easily get the original image. The complete algorithm is given as follows:

Step 1. Decompress the location map using JBIG1 and partition it into two equal sized segments to obtain location maps LM1 and LM2.

Step 2. Extract the secret data from all the interpolated pixels as follows:

```
If bit of the location map is '1' and the corresponding pixel is even valued,
    Add '1' as the secret data bit and increase the pixel value by one
Else if the location map is '1' and the corresponding pixel is odd valued add
    Add '0' as the secret data bit.
Else
    Do nothing.
End
```

Step 3. Extract the secret data from all the interpolated pixels as follows:

```
If bit of the location map is '0' and the corresponding pixel is odd valued,
    Add '1' as the secret data bit and decrease the pixel value by one
Else if the location map is '1' and the corresponding pixel is even valued add
    Add '0' as the secret data bit.
Else
    Do nothing.
End
```

Step4: XOR the obtained secret using the private key to obtain the original secret data.

Step5: Thus, we obtain the original cover image and complete hidden secret data.

B. *Experimental Results and Discussions*

In this section, we carry out experiments by taking most widely used images for evaluating their performances. The image quality metrics used are Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). The reason of using MSE and PSNR as quality metrics in our experiments is that these are the most widely used in the literature. The data hiding capacity is calculated in bytes.

In this section, we calculate these parameters for our proposed scheme and compare them with that of the very important reversible data hiding scheme [25, 30]. We have taken nine images as the cover media for covering the variance in the image characteristics. We have implemented the proposed scheme in MATLAB running on the Intel® Core 2 Duo 2.20 GHz CPU, and 3GB RAM hardware platform. The secret data to be embedded is generated using random function. The proposed scheme increases the embedding capacity by embedding the secret data into two passes as in the first pass it embeds one bit of the secret data into every even valued pixels by either increasing its value by one or leaving it unchanged and in the second pass in every odd valued pixel by either decreasing their value by one or leaving them unchanged. Thus, it makes some of the even valued pixels odd in the first phase which will again be used to embed the secret. The results based on the PSNR values and hiding capacities in bits for different data hiding techniques are illustrated in Table 3 & 4.

Table 3: A comparison of Jung &Yoo's scheme on capacity with the proposed scheme

Images	Jung and Yoo's method [25]	Chang's method [30] (A)	Proposed method (B)	Percentage increment ((B-A)/A)
Lena	235460	247095	328052	32.76
Boat	226159	269431	327849	21.68
Jelly beans	236545	256974	328605	27.87
Tiffany	202238	227822	327837	43.90
Couple	268389	258555	327603	26.70
Baboon	460740	396651	327680	-17.38
Man	256987	278954	327899	17.54
House	246595	259635	328067	26.35
Splash	236595	256935	327517	27.47

The results for the proposed data hiding scheme are compared with some of the popular schemes like Jung &Yoo method [25] and Chang et al. method [30]. The comparison in terms of data hiding capacity and visual quality are illustrated in the Table 3. From the table 4, it is clear that the proposed scheme is superior in terms of both the data hiding capacity and visual quality to the existing schemes except the case of baboon. In fact, it gains the increment in the PSNR value in the range of 19.98 to 56.38 and in the data hiding capacity in the range of 17.54 to 43.90% (except baboon image) with respect to Chang et al. method [25]. We have calculated the increment percent with respect to Chang et al. method [25] because its performance is better than the Jung &Yoo method [30] in terms of both the data hiding capacity and image quality.

Table 4: A comparison of Jung &Yoo's scheme on PSNR with the proposed scheme

Images	Jung and Yoo's method [25]	Chang's Method [30] (A)	Proposed method (B)	Percentage increment ((B-A)/A)
Lena	30.61	43.61	54.1514	24.17

Boat	28.62	41.12	54.1675	31.73
Jelly beans	31.56	36.56	54.2248	48.31
Tiffany	32.02	45.15	54.1724	19.98
Couple	30.88	43.40	54.1674	24.80
Baboon	23.13	34.63	54.1558	56.38
Man	29.36	40.56	54.1725	33.56
House	30.59	35.63	54.1749	52.04
Splash	31.89	38.93	54.1499	39.09

In case of baboon, our scheme is performing with the same standard as in case of other images but the Chang et al. scheme is performance is outlier as it is the noisiest image. In fact, the proposed scheme performs equally well for all the cover images irrespective of their characteristics. Our scheme provides better quality stego-image because the proposed hiding scheme does not make major changes to the pixel values while embedding the secret data. In fact, it only changes the pixel values at most by 1 which is a very minute change. Our proposed scheme has achieved more than 54 db PSNR for entire group of images irrespective of their characteristics.

V. CONCLUSION

In this paper, we have introduced two reversible data hiding scheme using image interpolation. In the first scheme, we have proposed a new reversible data hiding method based on image interpolation and pixel intensity. The method can hide the secret data into both color as well as gray scale images. This approach also supports the any format of the image. Our method also increases the security of the secret data as it XORes it with a secret key before hiding. Furthermore, it is less computationally complex because it does not make much computation, it only check pixel intensity and embeds the secret data. The quality of the obtained stego-image is better with significant hiding capacity. The method only hides the secret data into the scaled up pixels. The experimental results show that our proposed method achieves higher data hiding capacity with higher PSNR values.

In the second scheme, we have proposed an image interpolation based reversible data hiding scheme using complementary strategy. This scheme's data hiding phase embeds the secret data into two passes. In the first pass, it embeds the secret data into the even valued pixels either by increasing their value by one or leaving them unchanged based on the secret data bit. In the second pass, the secret data is embedded into the odd valued pixels either by decreasing their value by one or by leaving them unchanged. Thus embedding, the maximum change made to a pixel can be 1 which is very minute. Furthermore, some of the pixels utilized for embedding in the first pass, are gain used for the embedding in the second pass as their values has changed in the first pass embedding which helps in increasing the embedding capacity. Thus, our scheme is able to provide a good quality stego-image and achieve high data hiding capacity.

References

[1] Stefan Katzenbeisser and Fabien A. P. Petitcolas "Information Hiding Techniques for Steganography and Digital Watermarking" ARTECH HOUSE, INC. 685 Canton Street Norwood, MA 02062, pp. 1-9.

[2] M. Al-Husainy "A New Image Steganography Based on Decimal-Digits Representation", Computer and Information Science, vol. 4, no. 6; November 2011

[3] N. Tiwari and M. Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and Its Applications Vol. 4(4), Oct. 2010.

[4] S.P. Maity, M.K. Kundu, P.K. Nandi, Genetic algorithm for optimal imperceptibility in image communication through noisy Channel, in: Proceedings of the International Conference on Neural Information Processing (ICONIP '2004), India, 29 October 2004, pp. 700–705.

[5] Al-Haidari, F., Gutub, A., Al-Kahsah, K., Hamodi, J., Improving security and capacity for arabic text steganography using 'Kashida' extensions. In: The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA – 2009), Rabat, Morocco, May 10–13, pp. 396–399, 2009.

[6] Gutub, A., Fattani, M., A novel arabic text steganography method using letter points and extensions. In: WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria, May 25–27, pp. 28–31, 2007.

[7] I.C Lin, Y.B Lin, C.M Wang "Hiding data in spatial domain images with distortion tolerance", in Computer Standards & Interfaces, Vol.31, 2009, pp.458–464.

[8] C.K Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, 2004 ,pp.469 – 474.

[9] C.H Yang, C.Y, Weng, S.J Wang, H.M Sun, "Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems", in The Journal of Systems and Software, Vol.83, 2010, pp.1635–1643.

[10] C.C. Chang, T.C. Lu, "A difference expansion oriented data hiding scheme for restoring the original host images", Journal of Systems and Software, Elsevier, Vol. 79, 2006, pp.1754–1766.

[11] A.M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", in IEEE Transactions on Image Processing, Vol.13, 2004, pp.1147–1156.

[12] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, 2003, pp.890–896.

[13] B.Yang , M. Schmucker, W.Funk , C. Brush , S. Sun, "Integer DCT-based reversible watermarking for images using companding technique", in Proc. of Int. J. Electron. Commun, vol.65 ,2011, pp.814– 826.

[14] G.Xuan , YQ. Shi, Q.Yao, Z. Ni, C.Yang, and J.Gao, "Lossless data hiding using histogram shifting method based on integer wavelets", in international Workshop on Digital Watermarking, Lecture Notes in Computer Science , 2006, pp 323–32.

[15] Z.M. Lu, J.X. Wang, B.B. Liu, "An improved lossless data hiding scheme based on image VQ-index residual value coding", Journal of Systems and Software , Vol.82, 2009, pp.1016–1024.

[16] C.C. Chang, C.Y. Lin, Y.H. Fan, "Lossless data hiding for color images based on block truncation coding", Pattern Recognition Vol.41, 2008, pp.2347–2357.

[17] Chi-Kwong Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution" Pattern Recognition, vol. 37, pp. 469 – 474, 2004.

[18] R.Z. Wang. C.F. Lin and J.C. Lin., "Image hiding by optimal LSB Substitution and genetic algorithm." Pattern Recognition, vol,34,671-683,2001

[19] CC. Chang, J.Y. Hsiao and C.S. Chan, " Finding Optimal LSB Substitution in Image Hiding by Dynamic Programming Strategy," Pattern Recognition, vol. 36(7),pp. 1583-1595,2003

[20] H.C. Wu. N.I. Wu. C.S. Tsai and M.S. Hwang, " Image Steganographic scheme based on pixel value differencing and LSB replacement methods," IEE Proc. Vision Image Signal Process, Vol, 152,pp,611-615,2005

[21] Seung-Won J, Le Thanh H, Sung-Jea K (2011) A New histogram modification based reversible data hiding algorithm considering the human visual system. IEEE Signal Processing Letters 18(2): 95–98

[22] Tai W-L, Yeh C-M, Chang C-C (2009) Reversible data hiding based on histogram modification of pixel differences. IEEE Transactions on Circuits and Systems for Video Technology 19(6): 906–910

[23] Chang CC, Lin CY (2007) Reversible steganographic method using SMVQ approach based on declustering. Information Sciences 177(8):1796–1805

[24] T. M. Lehmann, C. Gonner, and K. Spitzer, "Survey: Interpolation methods in medical image processing", IEEE Trans. on Medical imaging, vol. 18(11), 1999.

[25] K. H. Jung and K.Y. Yoo, "data hiding method using image interpolation", computer standard and interfaces, vol. 31(2), pp. 465-470, 2009.

[26] Jan SR, Hsu SJ, Chiu CF, Chang SL, "An improved data hiding method using image interpolation", in : 2011 seventh international conference on intelligent information hiding and multimedia signal processing, pp, 185-188.

[27] Yalman Y, Akar F, Erturk I, "an image interpolation based method reversible data hiding method using R-weighted coding" in 2010: 13th IEEE international conference on computational science and engineering, pp 346-350.

[29] CF Lee, YL Huang, "An efficient image interpolation increasing payload in reversible data hiding", Expert System Application 39: 6712-6719.

[30] Ya-Ting Chang et al., "Image interpolationg based data hiding in conjunction with pixel shifting histogram", Journal of supercomputing. Springer 66:1093-1110, September 2013

[31] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, 2004.

[32] R. Chandramouli and N. Memon, "Analysis of LSB based Image Steganography Techniques", Proceedings of ICIP 2001, Thessaloniki, Greece, October 7−10, 2001.

[33] CC. Chang, J.Y. Hsiao and C.S. Chan, " Finding Optimal LSB Substitution in Image Hiding by Dynamic Programming Strategy", Pattern Recognition, vol. 36(7),pp. 1583-1595,2003

[34] H.C. Wu., N.I. Wu., C.S. Tsai and M.S. Hwang, " Image Steganographic scheme based on pixel value differencing and LSB replacement methods", IEE Proc. Vision Image Signal Process, Vol, 152, pp. 611-615, 2005

[35] H. B. Kekre, A. Athawale, P. N. Halarnkar, "Performance Evaluation of Pixel Value Differencing and Kekre's Modified Algorithm for Information Hiding in Images", International Conference on Advances in Computing, Communication and Control, 2009 pp 342-346