International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 274 – 280

Data Security using Reversible Data Hiding with Optimal Value Transfer

Mrs. Darshana N. Tambe
Assistant Professor
PVPPCOE/Dept. of IT, Mumbai, 400022, India
Janudarshana9@gmail.com

Abstract: In this paper a novel reversible data hiding algorithm is used which can recover image without any distortion. This algorithm uses zero or minimum points of an image and modifies the pixel. It is proved experimentally that the peak signal to noise ratio of the marked image generated by this method and the original image is guaranteed to be above 48 dB this lower bound of peak signal to noise ratio is much higher than all reversible data hiding technique present in the literature. Execution time of proposed system is short. The algorithm has been successfully applied to all types of images.

*****

I. INTRODUCTION

Reversible Data Hiding

Nowadays, with the rapid development of information technology more and more images and data are available on the internet. So there is a need to provide some kind of authentication to such important data. When the sender transmits the image to the receiver, there may be intruders present in between who may capture the image. After capturing the image the image the intruder may view the meaningful content in the image. This may not be the problem in some cases. But if we consider medical and military images then such distortion is unacceptable.

Data hiding technique aims to embed some secret information into a carrier signal by altering the insignificant components for copyright protection or covert communication. In general cases, the data hiding operation will result in distortion in the host signal. However, such distortion, no matter how small it is, is unacceptable to some applications, e.g., military or medical images. In this case it is imperative to embed the additional secret message with a reversible manner so that the original contents can be perfectly restored after extraction of the hidden data. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types:

1. Lossless compression based methods
2. Difference expansion (DE) methods
3. Histogram modification (HM) methods

Watermarking technique can be classified into two different types.

In the first type the watermark is visible i.e. different logos or text can be inserted which is visible. This technique can be seen in Microsoft MS Word where we apply watermarks on the pages which are visible.

The second technique used for applying watermarks to the images, videos, is invisible. This invisible technique is called as digital watermarking. The digital watermarking technique can be used for a wide range of applications, like for providing copyright protection to the films, videos, etc. The digital watermark is a more secured technique because the watermark is not visible, So if the intruder view the content of the image he will not be aware of the watermark which is already present in the image. So if the intruder performs any modification in the image it will be known to the receiver after receiving the image. The receiver after receiving the image will see that the watermark has been changed and will be aware that the image has been modified.

The watermarking technique can be made more secure by encrypting the watermarked image. Various methods of encryption can be used to encrypt the image. Encryption is a technique by which the image is changed or modified by using keys. The encryption technique can be classified into two type's i.e. symmetric key encryption in which the same key is used for encryption and decryption and asymmetric key encryption in which different keys are used for encryption and decryption. Sender will use the public key for encryption and receiver will use the private key for decryption. But whatever technique is used, the original quality of the image must be recovered at the receiver i.e. the receiver must get the original image after removing the watermark and after decrypting the encrypted image.

Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten. This would make the images acceptable for legal purposes. Reversible data hiding (RDH) has the capability to erase the distortion introduced by embedding step after cover restoration. It is an important

property that can be applied to many scenarios, such as medical imagery, military imagery and law forensics. For this reason, RDH becomes a hot research topic and is extensively studied over the years. Reversible data hiding (RDH) in images is a technique, by which the original cover can be lossless recovered after the embedded message is extracted.

DATA HIDING is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication, however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as *reversible*, *lossless*, *distortion-free*, or *invertible* data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be lossless recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.

This technique first segments an image into no overlapping blocks, and then introduces a discriminating function to classify these blocks into three groups: R (regular), S (singular), and U (unusable). It further introduces a flipping operation, which can convert an R-block to an S-block and vice versa. A U-block remains intact after the flipping operation. By assigning, say, binary 1 to an R-block and binary 0 to an S-block, all R- and S-blocks are scanned in a chosen sequential order, resulting in a biased (meaning that the binary numbers of 1 and 0 are not balanced) binary sequence. This biased binary sequence is losslessly compressed to leave space for data embedding and the compressed bit sequence is embedded into the cover media as an overhead for later reconstruction of the original image. In data embedding, the R- and S-blocks are scanned once again and the flipping operation is applied whenever necessary to make the changed R- and S-block sequence coincident with the to-be-embedded data followed by the overhead data mentioned above. While it is novel and successful in reversible data hiding, the payload is still not large enough for some applications. Specifically, the embedding capacity estimated by author's ranges from 3 to 41 kb for a 512 x512x 8 cover gray scale image when the embedding amplitude is 4 (the estimated average PSNR of the marked image versus the original image is 39 dB).

Another problem with the method is that when the embedding strength increases in order to increase the payload, the visual quality of the marked image will drop severely due to annoying artifacts. To increase the payload dramatically, a new lossless data hiding technique based on integer wavelet transform (IWT), (a second generation wavelet transform, which has avoided round-off errors) was developed recently. Because of the superior decor relation capability of wavelet transform, the selected bit plane compression of IWT coefficients in high frequency sub bands creates more space for data hiding, resulting in a two to five times payload as large as that in. Specifically, its payload ranges from 15 to 94 kb for a 512 x512 x8 gray scale image at the same (39 dB) PSNR of the marked images compared with the original images. To achieve reversible data hiding, a histogram modification is applied in its pre-processing to prevent over/underflow. This histogram modification causes, however, a relatively low PSNR of the marked image versus the original image though there are no annoying artifacts. It is noted that reversible data hiding has attracted increasing attention recently, and more algorithms are being developed.

The main idea is that in the embedding phase, the host signal is quantized and the residual is obtained. Then the authors adopt the CALIC lossless image compression algorithm, with the quantized values as side information, to efficiently compress the quantization residuals to create high capacity for the payload data. The compressed residual and the payload data are concatenated and embedded into the host signal via generalized-LSB modification method. The payload of this technique is from 15 to 143 kb for a 512x512 x8 gray scale image while the PSNR is 38 dB. Even though the payload is high, the PSNR is still not high enough. In this paper, we propose a new reversible data embedding technique, which can embed a large amount of data (5–80 kb for a 512x512x8 gray scale image) while keeping a very high visual quality for all natural images, specifically, the PSNR of the marked image versus the original image is guaranteed to be higher than 48 dB. It utilizes the zero or the minimum point of the histogram (defined below) and slightly modifies the pixel gray scale values to embed data. This technique can be applied to virtually all types of images. Up to now, it has been successfully tested on different types of images, including some commonly used images, medical images, texture images, aerial images, and all of the 1096 images in Corel DRAW database. The computation of our proposed technique is quite simple and the execution time is rather short. Although the proposed lossless data hiding technique is applied to still

images, it is also applicable to videos which consist of a sequence of images.

II. PREVIOUS WORK

Losles Generalized-Lsb Data Embedding

Mehmet UtkuCelik, , Gaurav Sharma, Ahmet Murat Tekalp and Eli Saber [2] presented a reversible data-hiding technique. That technique enables the exact recovery of the original host signal upon extraction of the hidden information. A generalization of the well- known least significant bit (G-LSB) modification is used as the data-embedding method. This method introduces additional operating points on the capacity-distortion curve. The reversible losel's recovery of the original is achieved by compressing portions of the host signal that are susceptible to embedding distortion and transmitting this compressed portion as a part of the embedding payload. A prediction-based conditional entropy coder who utilizes unaltered portions of the host signal as side-information improves the compression efficiency and, thus, the reversible data-embedding capacity. In this well-known method, the LSB of each signal sample is replaced (over written) by a payload data bit embedding one bit of data per input signal sample. If extra capacity is required, two or more LSBs may beover written allowing for a corresponding bit per input
Signal sample. During extraction, these bits are reading in the same scanning order, and payload data is extracted. LSB modification is a simple, no robust embedding technique with a high-embedding capacity and small bounded embedding distortion (±1).

Reversible Data Embedding Using A Difference Expansion

In the difference expansion method differences between two adjacent pixels are doubled so that a new LSB plane without carrying any information of the original is generated. The hidden message together with a compressed location map derived from the property of each pixel pair, But not the host information itself, is embedded into the generated LSB plane. Jun Tian introduced a DE technique [DE], which discovers extra storage space by exploring the repletion bits in the image content. They employed the DE technique to reversibly embed a payload into digital host images. Both the payload embedding capacity limit and the visual quality of embedded images of the DE method are among the best in the literature, along with a computational complexity is low.

Reversible Watermark Using The Difference Expansion Of A Generalized Integer Transform

Adnan M. Alatar used; a reversible watermarking algorithm with very high data-hiding capacity has been developed for color images. The algorithm hides several bits in the difference expansion of vectors of adjacent pixels. Also, the potential payload size capacity that can be embedded into a host image is discussed, and a feedback system for controlling this size is developed. The recursive embedding and embedding across color components to hide more data into a host image was used to hide more payloads.

Spatial Triplets: A spatial triplet is a 1 X 3 or 3 X 1 vector formed from three consecutive pixel values in the same color component from the row- or column-wise, respectively. We applied this algorithm recursively to each color component: first o the columns and then to the rows.

Spatial Quads: A spatial quad was assembled from 2 X 2 adjacent pixels in the same color component. We applied the algorithm to each color component independently.

Cross-Color Embedding: To hide even more data, the algorithm can be applied across color components after it is applied independently to each color component either in row or column wise. In this case, the vector u contains the color components (R,G,B) of each pixel arranged in a predefined order. This cross-color application can be done either as cross-color Triple u=(R,G,B) , as cross-color quad u=(R,G,G,B) , or as a permutation thereof. The results indicate that the spatial, quad-based algorithm allows for hiding the largest payload at the highest signal-to-noise ratio. The amount of data can embed into an image depends highly on the nature of the image. This is the main drawback of this method.

Data Hiding Exploiting Spatial Correlation between Sub-Sampled Images

Reversible data hiding enables host media to be restored from marked media without any loss of original host information, because this reversibility algorithm helps to make a right decision during image analysis, it is highly desirable in quality-sensitive imagery where even the minimal distortion introduced by embedding data is unacceptable. K-.S.Kim, M.-J.Le, H.-Y.Le, and H.-K.Le used a reversible data hiding method that modifies the histogram difference between sub-sampled images of original host data. It exploits the high spatial correlation inherent in neighboring pixels to achieve high capacity and imperceptible embedding. This section presents a histogram-based reversible data hiding method for images in spatial domain, which satisfies high embedding capacity,high visual quality, and low computational complexity.

Reversible Data Hiding With Optimal Value Transfer

In Xinpeng Zhang used the practical reversible data hiding scheme for perfectly restored the original content after extraction of the hidden data. That is the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure. The secret data, as well as the

auxiliary information are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors. Here, the optimal value transfer rule is used to modify the estimation errors. The optimal value transfer matrix is produced for maximizing the amount of secret data, i.e., the pure payload, by the iterative procedure. Also, the host image is divided into a number of pixel subsets and an estimation error in the next subset is always embedded by the auxiliary information of a previous subset.

A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an reverse order. In this way, a god reversible practical data hiding performance is achieved. This way, a god payload-distortion performance can be achieved. In other words, the optimal transfer mechanism gives a new rule of value modification and can be used on various cover values. A better performance is achieved, if a smarter prediction method is exploited to make the estimation errors closer to zero, but the computation complexity is higher due to the prediction and iterative procedure. This is the major drawback of this method.

Spatial Domain Data Hiding Techniques

Spatial domain technique based data hiding involve manipulation of pixel values and has commenced since the early 1980‘s with Ingemar J. Cox et al technique (1997) for secure spread spectrum watermarking (SSSW) for multimedia which has the property of tamper resistance followed by Jiri Friedrich (1998), who has utilized the complementary robustness properties of both low frequency watermarks and spread spectrum generated watermarks to obtain a watermarked image capable of surviving an extremely wide range of severe image distortions. AthanasiosNikolaidis et al. (2001) technique is a region based watermarking where the robust regions are carefully selected through preprocessing stages utilizing segmentation and clustering. Acharya et al. (2004) have utilized the least significant bit replacement concept to perform the embedding of electronic patient information inside the medical image. Hsien et al. (2005) provided a vector quantization based method to reduce the storage and transmission time. Celik et al. (2005) technique is based on a least significant bit replacement with the bits of the payload.

Giakoumaki A., et al. (2004) and Alessia De Rosa et al. (2006) have discussed the authentication and labeling of medical images through data hiding for health care management which forms the motivation behind this work. Navneet Mandhani et al. (2005) have introduced a code division multiple access scheme for hiding data in monochrome images. Huang et al. (2005) have suggested chrominance utilization based watermarking technique, where the payload is inserted into the directional coefficient values of the color image and the results show good perceptual invisibility and robustness towards filtering, compression and cropping. Neminath et al. (2009) utilized the histogram of images to develop a watermarking technique found to exhibit a good fidelity. Osamah Al – Qershi et al. (2009) have suggested a region of interest (ROI) based data hiding in medical images and is shown to be tamper resistant. A recent advancement in the spatial domain methods are the utilization of luminance values of an image proposed by Jamal Hussein (2010) which exhibited good tolerance towards JPEG compression and rotation attacks. Chin Feng Lee et al. (2011) have put forward reversible data hiding technique utilizing a vector quantization compression code and is able to restore the original image without any distortion.

Frequency Domain Data Hiding Techniques

Even though the above mentioned spatial domain techniques provide a good fidelity, the quality of image tends to degrade with increasing aggressive image processing operations such as increased compression, scaling, filtering and increased levels of noise as spatial domain techniques tend to operate on raw pixel values as such. Normally the transformation divides the image into high frequency and low frequency components with mid band frequency components in between. This decomposition or separation of frequencies also provides the user increased flexibility in choice of an ideal embedding location depending on the application. If the watermarked image tends to be compressed during its path, the watermarks could be embedded into the low or mid frequency components. On the other hand, if the watermarked image tends to be passed through a channel prone to high levels on noise, then it is desirable to embed in the low frequency components of the image. The heart of any frequency domain watermarking is the transform used for decomposition and reconstruction.

Many transforms exist such as the Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Contourlet Transform (CT), Curvelet Transform, Ridgelet Transform (RT), Shearlet Transform (ST) etc., Choice of appropriate transform for specific application is truly a challenge to obtain optimal embedding results due to unique properties of different transforms.

The mid band coefficients of a DCT transformed host image are chosen to be the embedding location for embedding a pseudo random sequence corresponding to the payload in the technique proposed by Mauro Barni et al. (1998). The resulting watermarked image proves to be robust towards aggressive image processing operations like compression, medial filtering etc., DeepaKundar et al. (1998) have utilized the multi-resolution properties of the wavelet transforms for data hiding using a blind algorithm for extraction. Shinfeng et al. (2010) have reported a robust DCT based data hiding technique which exhibits a high degree of robustness towards a wide range of aggressive image processing operations. Another blind approach was developed by Jian Guo Cao et al. (2001), using a

redundant wavelet transforms which was adapted to the features of the cover image. An optimal recovery of watermark which was noise corrupted was proposed by Nam Yong et al. (2001) utilizing the wavelet vaguelette decomposition (WVD) along with wavelet shrinkage. Wang et al. (2002) technique is based on the DWT and is proved to have good robustness towards certain image processing operations simulated for real time attacks. Xuan et al. (2002) technique is based on conversion of spatial domain image into the frequency domain by utilizing the integer wavelet transform which is found to show satisfactory robustness towards certain types of attacks.

Hybrid Transforms For Data Embedding

Hybrid transforms are unique in nature and it can be rightly justified by observing the properties of them in the following sections. Since, efficiency of a data embedding system is all about finding the optimal tradeoff between robustness, perceptual invisibility and embedding capacity, the essential properties of different transforms discussed in the previous sections have been combined in a hybrid combination to address the optimality criteria to the maximum extent possible. In line with this concept, many techniques have been put forward which have shown to exhibit performance features. Frank et al. (1999) have introduced a watermarking scheme to increase the watermarking capacity and also to provide a double kind of protection to the watermarking through his watermark splitting approach. KouroshJafari-Khouzani et al. (2005) technique combines DWT and SVD in a hybrid combination and is robust towards rotation, scaling and translation attacks. A hybrid combination of DWT and DCT by Ali Al – Haj et al. (2007) and visual model based DCT and DWT proposed by Ahmed A. Abdulfetah (2010) have shown robustness towards compression attacks while a combinatorial DWT and SVD approach by Gaurav Bhatnagar et al. (2009) have shown visual invariance towards scaling and translational attacks. The hybrid combinations of Contourlet transform and SVD to address the robustness issues and invariance towards RST attacks proposed by Venkatanarasimhulu et al. (2011) provide an effective motivation and platform to exploit the directional feature of the Contourlet transform and also to check the compatibility of the Contourlet transform towards other transform in a hybrid combination.

Ki - Hyun Jung et al. (2009) technique uses a interpolation technique to embed the watermark bits which is found to increase the embedding capacity and also the signal strength. Although, the signal strengths reported using this technique are slightly higher than 36 dB, its applicability to medical image with composite payload might prove to lossy. Jonathan Dautrich et al. (2009) utilize a difference expansion method for Minimizing Corrective Data so as to increase the embedding capacity with minimal errors. The approach presented here identifies pairs that do not need to have a bit in the location map, and constructs a reduced size selection vector in an attempt to increase the amount of embedding space that can be used by the payload. One of the major drawbacks to the difference expansion method is its apparent susceptibility to detection.

III. METHODOLOGY

The drawback of existing system is overcome by our proposed system.. In our proposed system we scramble the image first and then we hide the data within the image. This process provides enhanced security and protects the data from the intruder.

Image Scrambling and data hiding process proceeds in following 3 steps:

1.Authentication using AES.
2.Image Scrambling using Rubik's Cubic.
3.Embedding the data using Optimal Value Transfer Algorithm.

Existing System

A data-hider can also employ histogram modification mechanism to realize reversible data hiding. In the host image is divided into blocks sized 4 ×4, 8 ×8, or 16 ×16, and gray values are mapped to a circle. After pseudo-randomly segmenting each block into two sub-regions, rotation of the histograms of the two sub-regions on this circle is used to embed one bit in each block. On the receiving side, the original block can be recovered from a marked image in an inverse process. Payload of this method is low since each block can only carry one bit. Based on this method, a robust lossless data hiding scheme is proposed, which can be used for semi-fragile image authentication.

A typical HM method presented for utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel gray scale values to embed data into the image. In binary tree structure is used to eliminate the requirement to communicate pairs of peak and zero points to the recipient, and a histogram shifting technique is adopted to prevent overflow and underflow. The histogram modification mechanism can also be implemented in the difference between sub-sampled images and the prediction error of host pixels and several good prediction approaches have been introduced to improve the performance of reversible data hiding.

Disadvantages of Existing System

1. In these reversible data hiding methods, a spare place can always be made available to accommodate secret data as long as the chosen item is compressible, but the capacities are not very high.

2. Payload of this method is low since each block can only carry one bit.

Proposed System

Our proposed reversible data hiding technique is able to embed about 5–80 kb into a 512 512 8 gray scale image while guaranteeing the PSNR of the marked image versus the original image to be above 48 dB. In addition, this algorithm can be applied to virtually all types of images. In fact, it has been successfully applied to many frequently used images, medical images, texture images, aerial images, and all of the 1096 images in the CorelDraw database. Furthermore, this algorithm is quite simple, and the execution time is rather short. Therefore, its overall performance is better than many existing reversible data hiding algorithms. It is expected that this reversible data hiding technique will be deployed for a wide range of applications in the areas such as secure medical image data systems, and image authentication in the medical field and law enforcement, and the other fields where the rendering of the original images is required or desired.

Advantages of Proposed system

1. A smarter prediction method is exploited to make the estimation errors closer to zero, a better performance can be achieved, but the computation complexity due to the prediction will be higher.

2. The payload-distortion performance of the proposed scheme is excellent.

3. The host image is divided into a number of subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset.

4. This way, one can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order.

Reversible Data Hiding:

In reversible data hiding techniques, the values of sender image are modified. According to some constraints the original content of the image can be correctly restored after extracting the watermark data on the receiver side. According to this technique, the optimal constraint of value modification using a payload-distortion criterion is founded by using the iterative procedure, and a reversible practical data hiding scheme was proposed.

The secret watermark data, as well as the additional information used for recovering the content, were carried out by the differences between the original pixel-values and the corresponding values estimated from the neighbors.

In this, the errors estimated were modified according to the optimal value transfer rule. Also, the original image was divided into a number of subsets of the pixel and the additional information of the subset were always embedded into the errors estimated in the next subset. The receiver could successfully extract the content i.e. the embedded secret data and recover the original content of the image in the subsets with an inverse order.

According to this technique, a good performance is achieved for the reversible data hiding. According to the above scheme, the secret watermark data, as well as the auxiliary information used for content recovery, were carried out by the differences between the original pixel-values and the corresponding values estimated from the neighbors, and the estimation errors are modified according to the optimal value transfer matrix. The optimal value transfer matrix is produced for maximizing the amount of secret data, i.e., the pure payload, by the iterative procedure described in the previous section. It also stated that the size of auxiliary information would not affect the optimality of the transfer matrix. By pixel division in the original image into two different sets and a number of different subsets, the embedding of the data is orderly performed in the subsets, and then the auxiliary information of a subset is always generated and embedded into the estimation errors in the next subset. Similarly, the receiver could successfully extract the embedded secret data and could recover the original content in the subsets with an inverse order.

3.1 Authentication using AES:

Advanced Encryption Standard (AES) is the first step of the process.AES algorithm is used to provide encryption to the login credentials.

The AES design consists of the secret key, plain text, cipher block and the cipher text. A key length of 128 bit is applied on the plain text block and after the cipher block processing, the resulting 128 bit cipher text is obtained.

AES consists of 10 rounds for 128 bit key. There are 9 regular rounds out of the 10 rounds while the 10^{th} round is different. The round of cipher block processing includesShift Rows, Sub Bytes, Mix Columns and AddRoundKey. The inverse cipher rounds include Inverse ShiftRows, Inverse SubBytes, Inverse Mix Columns and AddRoundKey. Thus we obtain the cipher text which is in the encrypted form.

3.2 Image Scrambling using Rubik's Cubic Algorithm:

Image scrambling is the process of scrambling the host image to convert it into an unidentifiable form. The Rubik's cubic algorithm partitions the selected host image into lot of different 54 blocks and forms lot of different Rubik's cubes,where each Rubik's cube contains 54 blocks. Then the rotations are performed on these formed Rubik's cubes based on the rotation parameter. The rotation parameter, Rp is a 3 bit parameter, whose first bit will denote the plus or minus sign. The first bit value 1 of Rpindicates negative and value 0 of Rpindicates

positive. The remaining two bits represent 0 to 3 respectively according to the bit pairs 00, 01, 10, 11.For rotation of the Rubik's cube, the generation of pseudo random number is done for scrambling purpose. For this pseudo randomly generated numbers the rotations are assigned based on the Rp associated with them.

1.3 Embedding the data using Optimal Value Transfer Algorithm:

While embedding the data, the differences between the original pixel-values and the corresponding values of the host image is estimated from the neighbors is usedto carry the payload that is made up of the actual secret data to be embedded and the auxiliary information for originalcontent recovery. According to the optimal value transfer matrix, the auxiliary information is generated and the estimation errors are modified.
Initially, the host image is divided into a number of subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. Thus, successful extraction of the embedded secret data and recovering of the original content in the subsets with an inverse order can be done.

IV. SYSTEM DESCRIPTION

The process starts when a user logs in to the application.The authenticated user is allowed to access the application and the user the selects the host image into which the secret data needs to be embedded. The application then scrambles the image using the Rubik's cubic image scrambling algorithm and embeds the secret data into the scrambled image using the Optimal value transfer algorithm to form the marked image At the receiver side the reverse process is applied.

V. CONCLUSION

Our proposed reversible data hiding technique is able toembed about 5–80 kb into a 512 x 512 x 8 grayscale imagewhile guaranteeing the PSNR of the marked image versus theoriginal image to be above 48 dB. In addition, this algorithmcan be applied to virtually all types of images. In fact, it hasbeen successfully applied to many frequently used images,medical images, texture images, aerial images, and all of the1096 images in the CorelDraw database. Furthermore, thisalgorithm is quite simple, and the execution time is rathershort. Therefore, its overall performance is better than manyexisting reversible data hiding algorithms. It is expected thatthis reversible data hiding technique will be deployed for a widerange of applications in the areas such as secure medical imagedata systems, and image authentication in the medical field andlaw enforcement, and the other fields where the rendering ofthe original images is required or desired.

2. Future Enhancements

1. We implement various algorithms to decrease the distortion from the image to get secure & efficient data hiding technique.
2. Try to achieve the highest lower bound of the PSNR with a quite large data embedding capacity.

REFERENCES

[1] M.Goljan,J.Thdrich,andR.Du,"Distortion-freedata embedding," in Proc. 4th hit. Workshop on Information Hiding, Lecture Notes in Computer Science,2001,vol.2137, pp. 27-41.

[2] M.U.Celik,G.Sharma,A.M.Tekalp, and E. Saber, "Lossless generalized-LSB data embedding,"IEEE Trans. Image Process.,vol.14, no. 2, pp. 253-266, Feb. 2005.

[3] J.Fridtich,M.Goljan,andR.Du, "Lossless data embedding for all image formats," in Proc. Security and Watermarking of Multimedia Contents IV, Proc. SPIE, 2002, vol. 4675, pp. 572-583.

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

[5] A. M. Alaftar, "Reversible watermark using the difference expansion of a generalized integer transform,"IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147-1156, Aug. 2004.

[6] X.Wang,X.Li,B.Yang,andZ.Guo,"Efficient generalized integer transform for reversible watermarking," IEEE Signal Process. Lett., vol. 17, no. 6, pp. 567-570,2010.

[7] H.-C. Wu, C.-C. Lee, C -S Tsai, Y.-P. Chu, and H.-R. Chen, "A high capacity reversible data hiding scheme with edge prediction and difference expansion,"J. Syst. Softw., vol. 82, pp. 1966-1973,2009.

[8] 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.

[9] L.KamstraandH.J.A.M.Heijmans, "Reversible data embedding into images using waveletechniques and sorting,"IEEE Trans. Image Process., vol. 14, no. 12, pp. 2082-2090, Dec. 2005.

[10] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no.12, pp. 1673–1687, Dec. 1997

[11] F. Perez-Gonzlez and F. Balado, "Quantized projection data hiding," in Proc.IEEE Int. Conf. Image Process., vol. 2, Sep. 2002, pp. 889–892.

[12] Rheema Rhineand NikhilaT.Bhuvan, "Image Scrambling Methods For Image Hiding: A Survey

[13] J. Irvine and D. Harle, Data Communications and Networks: An EngineeringApproach. New York: Wiley, 2002.