International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 1291 – 1297

A Brief Review of RIDH

Dipak Khirade, Aishwarya Thakare, Manisha Rane, Ankita Morey, Monika Kale
Department of Computer Science and Engineering
P. R. Pote College of Engineering and Management
Amravati, Maharashtra, India
dipakhirade@gmail.com
aishthakare1234@gmail.com
manisharane62@gmail.com
moreankita8888@gmail.com
monikakale779@gmail.com

Abstract:-The Reversible image data hiding (RIDH) is one of the novel approaches in the security field. In the highly sensitive domains like Medical, Military, Research labs, it is important to recover the cover image successfully, Hence, without applying the normal steganography, we can use RIDH to get the better result.
Reversible data hiding has a advantage over image data hiding that it can give you double security surely.

Keywords:-*Reversible Image Data Hiding (RIDH), Key Modulation, PSNR, BWT Algorithm, SVM Classifier.*

*****

I. INTRODUCTION

The Reversible image data hiding (RIDH) starts with the term steganography firstly which means hiding any type of data inside the multimedia file like audio, video, image, etc. The main flaw of steganography is that the cover media is get damaged after recovering the embedded data successfully. The main motive of proposing the RIDH scheme is to develop a technique by which we can recover the embedded data without causing any harm to the cover media [1]-[3].
Data Hiding is the process to hide data (representing some information) into cover media. That is, the data hiding process links two sets, a set of the embedded data and another set of the cover media image. The relationship between these two sets characterizes different applications. A number of reversible data hiding techniques have been proposed, and they can be roughly classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods. In practical aspect, many RDH techniques have emerged in recent years[3]-[7].
Previously, the data RIDH mainly work in the non encrypted domain, that is, it embeds the plain text inside an image with the lossless compression technique. Since the lossless compression is useful indeed, embedding the plain text in the image is the lack of security.

Some of the related terminologies are:

A. Watermarking

The term "Digital Watermark" was proposed by Andrew Tirkel and Charles Osborne in December 1992 [5]. The first successful embedding and extraction of a steganographic spread spectrum watermark was performed in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin [5].

To provide a security, firstly the watermarking was used inside the carrier media which is the very basic model of security. Basically, the watermarking was developed to add the digital signature of the media product inside that media to make it authorized. It is used to verify the reality or integrity of the carrier signal or to show the personality of its owners. It is evidently used for tracing copyright violation and for banknote authentication. It does not change the size of the carrier signal.

B. Steganography

The first reported use of the steganoraphy was coined by Johannes Trithemius in 1499 in his *Steganographia* [2]. A work on cryptography and steganography is a revolutionary change. The messages to be hide are generally embedded inside the image, video, audio, file, etc. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some practical works of steganography that fails to be described the secret of forms of security through ambiguity, where the scheme of key system follows to Kerckhoffs's principle.

Steganography consists of the hiding of information inside the electronic media. Steganography includes electronic communications that may consist of steganographic coding within the transport layer, like a document, image, program or protocol. It is best to use the media files to hide data because it having a very large size to hide a big amount of data in it. Comparing with the other media, media files provide much flexibility to add data in it.

The improvement of steganography over cryptography is that the source secret message does not attract mind to itself as an object.The encrypted messages throws a challenge on the most of the intruders to get the message by applying various decryption algorithms on it. The steganography mainly concerned with the hiding and sending the message but the cryptography concerned with encrypting the message by a advance mechanism, providing a key, and hiding it into a media file.

II. SURVEY

There are various data hiding techniques developed in recent years that are as follows:

1) J. Tian proposed a method Reversible data embedding using a difference expansion [1].

Reversible data embedding is also known as lossless data embedding, which is embeds invisible data (which is known as payload) into a digital image in a reversible pattern. The original digital content can be completely restored in reversible. In this method, reversible data-embedding method for digital images. Analyze the redundancy in digital images to achieve very high embedding capacity, as well as keep the distortion less. For digital images, this method presented a simple and efficient reversible date-embedding method. Search the repetition in the digital fulfilled to obtain reversibility.

The drawbacks of the above scheme are:

- The method fails to recover the original image successfully.
- Data embedding capacity is very low.
- Computational complexity very little bit high.

2) J. Mielikainen proposed a scheme which uses pixel pair matching [2] and it is based on a pair of pixels as the embedding unit. The LSB of first pixel carries one bit of information and a binary function of the two pixel values carry another bit of information. This scheme can carry same amount of data (The bits can be embedded into) as LSB matching with fewer changes to cover image. The MSE of LSB for 1 bit per pixel is 0.5, while for LSBMR it is 0.375.[7]

OPAP[8] is an advancement of LSB substitution method and it is based on embedding error. It uses only one pixel as embedding unit. In this method, for a m-bit pixel, if message bits are embedded to the right-most r LSB's then other m-r bits are adjusted by a simple evaluation. These m-r bits are either replaced by the adjusted result or otherwise kept unmodified based on if the adjusted result offers smaller distortion.

This method having drawbacks like:

- Lower capacity of embedding data since it can be rely on the present LSB's in the cover image.
- Pixel to pixel computation needs to done which can make more distraction in the cover image.
- More computation can cause the method to be more costly to implement.

3) Advancement of LSB matching method is exploiting modification direction (EMD) proposed by X .Zhang and S. Wang[3], in which each (2n+1)-ary notational system is applied by n cover pixels and mostly only one pixel is increased or decreased by 1. The target11 message is transformed into a sequence of digits in the conventional system with an odd base. Then pseudo-randomly permute all carrier image pixels according to a generated key, and make its partition into a sequence of pixel-groups, each having n pixels. The method is successful to achieve better stego-image quality under the same data size than traditional LSB.

Diamond Encoding is an advancement of EMD method and it first divides the carrier image into non-overlapping blocks of two consecutive pixels and transforms the message to a series of K-ary digits. For each block a Diamond Characteristic Value (DCV) is calculated and one secret K-ary digit is concealed into DCV [9]. The DCV is modified to secret digit and it is done by adjusting pixel values in a block. This method is capable of hiding more secret data while keeping the stego-image quality degradation imperceptible.

The drawbacks of the above scheme are:

- It is less robust as the hidden data can be lost with image manipulation.
- The hidden data can be destroyed easily by simple attacks.

4) Z.Ni, Y.-Q.Shi, N.Ansari, and W.Su. Coined a method Reversible data hiding [4].

The scheme prediction based reversible steganographic is depending on image in painting. In this method distribution characteristics of the content of the image are selected according to their reference pixels. The partial differential equations method is used in Image painting that depends on intact the prediction process by the reference pixels. The

Secret bits are reversibly displaced to embed the histogram prediction error. During the abstraction operation, the same

reference pixel can be overworked to conduct the prediction, which sure the lossless recovery of the cover image.
Drawbacks of this method are as follows:

- Pixel by pixel work need more time to perform action.
- Adding more data to each pixel leads to noisy cover image
- Noisy image leads to damage the cover image.

5) X. Wang, C. Shao, X. Xu, and X. Niu state a method, Reversible data-hiding scheme for 2-D vector maps based on difference expansion [5].
Reversible watermarking is best for hiding data in 2-D vector maps because the distribution of data bits evolved by data hiding can be recovered after getting the hidden bits. This paper states two methods for hiding a data by using difference expansion. The first scheme is based on the adjacent coordinates of vertices where it takes the coordinates of the vertices as the carrying media and embeds the data into it by advancing the differences in the adjacent coordinates. This technique got the greater capacity to embeds with highly correlated coordinates. The second approach uses the Manhattan distances between the neighbour vertices as the carrying media. To get the Manhattan distances from the coordinates, they define a set of invertible integer mapping and then they embed the data by modifying the differences in between the adjacent distances. This approach shows better result than the first one, both in capacity and invisibility for those maps where distances pursues more correlation [3].
The drawbacks of this scheme are:

- This scheme did not display good visual quality for all frequencies of embedding capacity.
- This scheme needs side information to initiate extracting phase while these data are not embedded into the host image.
- This scheme show good performance only with smooth images, which make them suitable for specific types of images.
- This scheme is complicated and time consuming as it scans the host image more than once.

6) D.M.Thodi, J.J. Rodrı´guez coined a method Expansion embedding techniques for reversible watermarking [6].
Expansion embedding technique expands the prediction errors. The prediction errors are usually smaller than the difference between the two consecutive pixel values.it overcomes the two drawbacks of Tian's algorithm by using the histogram-shifting technique. One of them was the poor penetrability control and second was inconvenient distortion at less embedding capacities. It illustrates two new algorithms for reversible watermarking, difference expansion and combining histogram shifting: that are highly compressible overflow map and another one using the flag bits. The reversible data-embedding technique is also known as prediction-error expansion was then imported and on the basis of prediction-error expansion technique, watermarking algorithms were presented. The method offers better result than its predecessors which use difference expansion. Test outcome analyze the watermarked image quality (deliberate in PSNR)for a given pay load size for a variation of images establish the good performance of this recommended difference-expansion algorithms by Tian's algorithm.
The drawbacks of this method are:

- Method is not suitable for applications requiring high quality images.
- The compressibility of the overcrowding location map is stable unwanted in some types of image.

7) W. L. Tai, C. M. Yeh, and C. C. Chang coined a scheme Reversible data hiding based on histogram modification of pixel differences [7].
For secure communication, Reversible data concealing method is used for data hiding. In this approach, the private information is cached into a cover media by hardly at all converting its pixel values and the embedded message also the original cover image should be totally retrieved from the watermarked image. This approach can performed the image repetition better as well as obtain an improved exploit by already imported one dimensional histogram based methods. With the help of DPM, the number of pixels bring data is increased since the number of pixels used for replacing is decreased. In inclusion, a pixel pair choosing strategy is also maintaining. In this scheme to priory use the pixel pairs located in smooth image zone to embed data. The smooth image filed has low noisy level. This is coined to another enhance the embedding exploit.
The drawbacks of the above scheme are:

- Maintaining a data of image histogram is tough work.
- Changes in image properties can damage the image.
- Data embedding capacity is comparatively low.

8) Y. Hu, H. K. Lee, and J. Li proposed a method DE based reversible data hiding with improved overflow location map [8].
For DE that is difference expansion depends on reversible data
hiding, the embedded bit-stream is divided into two parts that are: first part that forward the private message and the other part that include embedding information, consists of the 2-D binary location map and the header file. The drawback of previous reversible algorithms generally have

limited embedding capacity and low image quality. With the development of embedding capacity and image quality, this technique is being considered not only for the complete spectrum of fragile watermarking, like a authentication watermarks or watermarks protecting the image integrity, but it also for transferring communication, even for some uncommon applications such as image or video coding.
Drawbacks of this approach are:

- Adding the high security leads to complex complexities.
- Watermarking can easily show the data embedded.

9) X. Zhang state a method Separable reversible data hiding in encrypted image [9].
A novel design for separable reversible data hiding, which includes image encryption data embedding as well as data extraction or image restoration states.
In the first state, using an encryption key encrypts the original uncompressed image by the content owner. When a data-hider does not know the original content, using a data-hiding key to build a rare space to consist of the further data, he can compress the least significant bits of the encrypted image. for another data, the receiver may extract the other data by using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. At the same time the receiver has both of the keys, if the amount of further data is too large, he can extract the remaining data and recover the original content but with any error by manipulate the spatial correlation in natural image. The lossless compression does not change the content of the encrypted image containing embedded data, because lossless compression method is used for the encrypted image containing embedded data, the further data can be still bring out and the starting content can be also recovered.
The drawbacks of this scheme are:

- Data compression is not efficient .

10)Xinpeng Zhang proposed the [10] Reversible data hiding with optimal value transfer. Here, he used secret data and valuable information to recover the content in the image. It can be calculated as the differences between the pixel values of the image. The values of the nearest pixel can be calculated from the adjacent pixels. The calculation errors are modified by to the optimal value transfer rule. By using another method, the image or text data can be added invisibly into a video based on Integer Wavelet Transform. The difference is the mean square value difference between the original and watermarked image. It can be used also to increase PSNR. Again, it can be used the method of RIDH that is, separable reversible data hiding in encrypted.The original uncompressed image get encrypted by using a encryption key, and the task can be performed by the content owner only. The LSB's of encrypted image may get compressed by a data hider. Finally, by using a data hiding key to generate a pixel difference to attach some additional data.
Some of the drawbacks of this scheme are:

- Additional storage into the image get wasted to store the additional data.
- Image distortion may get increased.

11) In [12] C. Anuradha and S. Lavanya coined a secure and authenticated discrete reversible Data hiding in cipher images. It works with security and authentication. First phase includes encryption of the original uncompressed image by a content owner. It uses an encryption key. After that a data hider can compress the LSB's of the encrypted image. It again uses a secret key to create a sparse space. It may use some unwanted data. It can encrypt image containing unwanted data. Receiver can extract that unwanted data by using that secret key. The receiver uses the image content for encryption and decryption. The receiver can decrypt the received data and can obtain the original like image by using that encryption key. He is unable to extract the additional data. If the receiver has both the data hiding key and the encryption key, Then it can extract the additional data as well as it can recover the original content without any error. It exploiting the exceptional data in natural image, when the amount of additional data is not too large.
This scheme pursues the drawbacks like:

- Limitation to the additional data.
- No action taken after exploiting the additional data.
- Additional data can leads to noisy image.

12) Afterwards, the researcher Wien Hong, Tung-Shou Chen [10] proposed a scheme Pixel Pair Matching (PPM) which can overcome the drawbacks of above schemes. This method uses the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The searched digit conceals the digit and it replaces the pixel pair. It makes use of a more compact neighborhood set than used in Diamond encoding. The extraction process finds the replaced pixel pair to extract the message data. Exploiting Modification Direction (EMD) method has a maximum capacity of 1.161 bpp and Diamond Encoding (DE) extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads [13].

This pursues the drawbacks like:

- Improper reconstruction of the cover image due to higher payloads.
- Extended work needs more complex computations than the previous method discussed.
- Higher amount of data needs superior type of cover image which leads to make the embedding and extraction process complex.

13) HaoTian Wu, JeanLuc Dugelay, And YunQing Shi proposed a method Reversible Image Data Hiding With Contrast Enhancement [13].
Reversible Image Data Hiding With Contrast Enhancement having advantage is Histogram and Location map gives the easy calculations. In this method a new reversible data hiding algorithm, has been coined with resources of contrast enhancement. For data embedding selected two peaks (that is highest two bins) in the histogram, hence histogram equalization can be concurrently implement by repeating the process. The image contrast can be build up by dividing an number of histogram peaks pair by pair demonstrate by experimental result. It is Compared with special MATLAB function, the visual quality of contrast images is bring out by this algorithm is better secured. Without any additional information the original image can be exactly recovered. Therefore the coined algorithm has made the image contrast enhancement reversible.
This scheme pursues the drawbacks like:

- Algorithm Robustness
- Having Poor visibility of image.

14) In the advancement, in 2001 the professors from Berlin, Heidelberg M. Goljan, J. J. Fridrich, and R. Du propsed a scheme called Distortion-free data embedding for images[6]. In this, they recover some drawbacks like one common drawbacks of all the embedding techniques are that they failed to recover the cover image as it is because it carries some distortion in it due to noise present just because of the data embeds itself. This distortion cannot be easily removed just because of the various available flaws like quantization, bit-replacement, or truncation at the grayscales 0 and 255. Even if the distortion is considered as very small, still it is unacceptable by the various organization like military, medical, research. In this paper, they introduce a general approach for high-capacity data embedding that is distortion-free (or lossless) in the sense that after the embedded information is extracted from the stego-image, they can revert to the exact copy of the original image before the embedding occurred. The new method can be used as a powerful tool to achieve a variety of non-trivial tasks, including distortion-free robust watermarking, distortion-free authentication using fragile watermarks, and steganalysis. The proposed concepts are also extended to lossy image formats, such as the JPG[6].
The drawback of this scheme are:

- The scheme failed to carry the maximum payload.
- The computational overload of the scheme is high enough to execute it smoothly.
- The reconstruction of the cover media again fails due to the over computational purpose.

.
15)The next is the histogram technique, proposed by Ya-Fen Chang and Wei-Liang Tai in 2012[11].
This technique includes developing histogram and finding the peak point and the zero point and shifting histogram bins to add source message bits. Later on, Ni et al. develops a reversible data hiding scheme, his scheme uses the histogram of an original cover image to add source messages. In this method, they found multiple pairs of peak and zero points, where a peak point denotes the pixel value with a maximum number of pixels in the cover image assume and a zero point corresponds to the pixel value with no pixel in the cover image assumes. It uses a pair of peak and zero points to embed the secret messages. P. H. Pawar et al.[13] uses histogram based RDH method. In this approach the cover image is divided into several equal blocks/tiles and then the histogram is generated for each of these blocks. Maximum and minimum points are computed for these histograms so that the embedding space can be generated to hide the data at the same time increasing the embedding capacity of the image. A one bit change is used to record the change of the minimum points. This improves the level of hiding places. This technique of block division successfully enhances the data hiding capacity because the total data that can be hidden in multiple blocks is generally larger than that can be hidden in a single cover image.
This scheme pursues the drawbacks like:

- Capacity is limited by the frequency of peak pixel value in the histogram.
- It searches the image several times, that makes the algorithm time consuming.

16) This paper is proposed for digital images, mainly focussed on grey scale images. Other algorithms just focus the PSNR values to keep high to enhance the contrast of an image, where this scheme improves the image quality as well as its security and lowers the bandwidth consumed. For adding data inside the image highest two peaks in the histogram are selected and then repeated the same process for performing histogram equalization. Using the chaotic encryption, the data is hided in the image, compressed and encrypted such that the data and image are completely recoverable. The proposed scheme was performed on two sets of images to prove its efficiency. It is found that, by

adding sufficient amount of data inside the image, the contrast of the image is being enhanced. It is proved that, this system works better than the three inbuilt MATLAB functions for contrast enhancement which as an add-on provides compression and encryption for better security.
The drawback of this scheme are:

- The data embedding capacity is lower.

17) The paper [9] proposes a novel scheme based on histogram shifting. The adjacent pixel values are almost similar in most of the cases, hence most of differences between pairs of adjacent pixels are equal or close to zero. In this scheme, a histogram is drawn based on these difference statistics. In the data hiding stage, a multilevel histogram modification technique is used. As more peak points are used for secret bits modulation, the hiding capacity is increased compared with other conventional methods based on one or two level histogram modification. As the differences concentricity around zero is improved, the distortions on the host image is seen by secret content embedding is mitigated. The data extraction and image recovery stage, the hiding level instead of the peak points and zero points is used. Since the affiliated information is much smaller than in those methods of the kind. Sequential recovery method is increased for each pixel is reconstructed with the aid of its previously recovered neighbor. The results and comparisons with other methods shows this method's efficiency and higher performance.
The drawback of this scheme are:

- The data embedding capacity is lower.
- Computational complexity increases.
- Exact recovery of cover image is tough task.

III. PROPOSED SYSTEM

The above discussed methods does not considered the image quality and image characteristics. The good method should must consider the image quality and attributes into consideration. Again, the security is the main concerned for the data to get hide inside the cover image which doesn't get focused into the above discussed approaches. In the sensitive areas like medical, military, research labs, it is important to recover the cover image without any loss of bits of cover image as well as the secret data.
Our proposed system focuses mainly on this three points to provide security as well as to reconstruct the original image.
The proposed system uses a powerful Burrows-Wheeler Transform (BWT) algorithm[1] which provides higher security to data before embedding into the cover image. The BWT is the algorithm which is uses to encrypt the normal message to convert it into the cipher text so that the intruder even if finds the way to extract the data from the image, still he will fails to get the original message. Transforming the data before embedding will give you the much security than above discussed methods and even reconstruction of cover images are useful in the sensitive domains.
At the decoder side, the hash function has been used instead of SVM classifier[1] which distinguish in between original image and the encrypted image. The key modulation concept will make the use of only the public key to encode and decode the data instead of private and public key mechanism which again reduces the computational complexities of the system

IV. CONCLUSION

This paper discussed the steganography techniques and then the various methods available for data embedding in a digital image. Comparative study for various methods is also provided. We discussed some of the widely used techniques, their methods of working and their limitations in brief. Finally, the proposed method has a capability to overcome all the discussed drawbacks of the previous methods. The proposed method can provide higher security, more data embedding capability, and perfect reconstruction of the cover image which the previously proposed techniques cannot achieve.

References

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[2] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.
[3] X .Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp.781–783,Nov.2006.
[4] Z.Ni,Y.-Q.Shi,N.Ansari,andW.Su,"Reversibledatahiding,"IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[5] X. Wang, C. Shao, X. Xu, and X. Niu, ``Reversible data-hiding scheme for 2-D vector maps based on difference expansion," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 311_320, Sep. 2007
[6] D.M.Thodi, J.J. Rodrı´guez,"Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing 16 (3)*,721–730,2007.
[7] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 6, pp. 906-910, Jun. 2009.
[8] Y. Hu, H. K. Lee, and J. Li, "DEbased reversible data hiding with improved overflow location map," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250 260, Feb.2009.
[9] Wu, Hao-Tian, and Jiwu Huang. "Reversible image watermarking on prediction errors by efficient histogram modification." *Signal Processing 92*, no. 12 (2012): 3000-3009.

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

[11] Wien Hong ,Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching*", IEEE transactions on information forensics and security*, Vol. 7, No. 1, February 2012.

[12] Xinpeng Zhang, Member, IEEE "Reversible Data Hiding With Optimal Value Transfer" *IEEE transactions on multimedia*, VOL. 15, NO. 2, FEBRUARY 2013.

[13] C. Anuradha and S. Lavanya "A secure and authenticated reversible Data hiding in encrpted images" © 2013, IJARCSSE

[14] HaoTian Wu, JeanLuc Dugelay, And YunQing Shi,"Reversible Image Data Hiding With Contrast Enhancement",*IEEE signal processing letters*, Vol. 22, NO. 1, January 2015.

[15] Anju Mariyam Zacharia, Shyjila P.A. and Karthika J S, "Compressed And Highly Secured Reversible Image Data Hiding With Contrast Enhancement", *International Journal of Informative & Futuristic Research*, Vol. 2, April 2015.

[16] M. Goljan, J. J. Fridrich, and R. Du, ``Distortion-free data embedding for images," in *Proc. 4th Inf. Hiding Workshop*, 2001, pp. 27_41.

[17] Ya-Fen Chang and Wei-Liang Tai "Histogram-based Reversible Data Hiding Based on Pixel Differences with Prediction and Sorting" *KSII Transactions on Internet and Information Systems*, Vol. 6, No. 12, Dec 2012.