ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Minimum Rate Prediction and Optimized Histograms Modification for Efficient Data Hiding

Anuja Bhondve, Prof. Swapnaja Suryawanshi

ME Computer Engineering, Dept. of Computer Engineering, Indira College of Engineering & Management, Pune, India

Asst. Professor, Dept. of Computer Engineering, Indira College of Engineering & Management, Pune, India

ABSTRACT: The process of retrieving the cover or host image without any damage after the secret data extraction is known as data hiding. The novel technique pixel prediction for PP (Pixel Prediction) based data hiding schemes based on the minimum rate criterion, which establishes the consistency in essence between the two steps of PP based data hiding schemes. Earlier PEE methods care for the two steps independently first either they focus on pixel prediction to obtain a sharp PE histogram, or second aim at histogram modification to enhance the embedding performance for a given PE histogram. Hence we are here proposing, a novel optimized histograms modification scheme to achieve the optimal embedding performance on the generated Random Pixel prediction sequence. The superiority of our method is verified through extensive experiments.

KEYWORDS: minimum rate prediction, Pixel Prediction (PP), data hiding (DH), optimized histograms modification, watermarked image.

I.INTRODUCTION

Data hiding is a technique used to put a secret data in a host images with small changes in host. In most of the data hiding schemes the cover image becomes distorted due to data hiding process and it cannot be retrieved back to the original form. Thus the cover media is permanently distorted due to the data embedding. In some applications, such as medical image processing and military image processing, retrieval of the original cover image without any damage is a must, since these images have too process further.

An information-hiding system is characterized using four different aspects: perceptibility, capacity, security, authentication, fingerprinting, secret communication, robustness and annotation [1] [2], etc. that all can be achieved by using data hiding techniques.

In most data hiding algorithms, the cover data is destroyed permanently and cannot be exactly restored after the embedded message is extracted. Recently, a new data hiding technique, namely, data hiding (RDH) [4] [5], is proposed, in which both the cover data and the embedded message can be extracted from the marked content. This specific data hiding technique has been found to be useful in the military, medical and legal fields, where the recovery of the original content is required after data extraction. It is also known as lossless activity.

Most of the proposed data hiding schemes are not base on pixel prediction and feature extraction. Reversible data hiding is also one of watermarking scheme which can be done in many ways like, Integer-to-Integer Wavelet Transform [6], Difference expansion [7], and Histogram modification [8].

Tian's DE algorithm is an efficient work of RDH. In DE algorithm, the host image is divided into pixel pairs, and the difference value of two pixels in a pair is expanded to carry one data bit. The original content restoration information, a message authentication code, and additional data will all be embedded into the difference values. By exploring the redundancy in the image, reversibility is achieved.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Ni et al. proposed a reversible data hiding method [9] based on histogram modification. In this method, each pixel value is modified at most by 1, and thus the visual quality of marked image is guaranteed. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel gray scale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms.

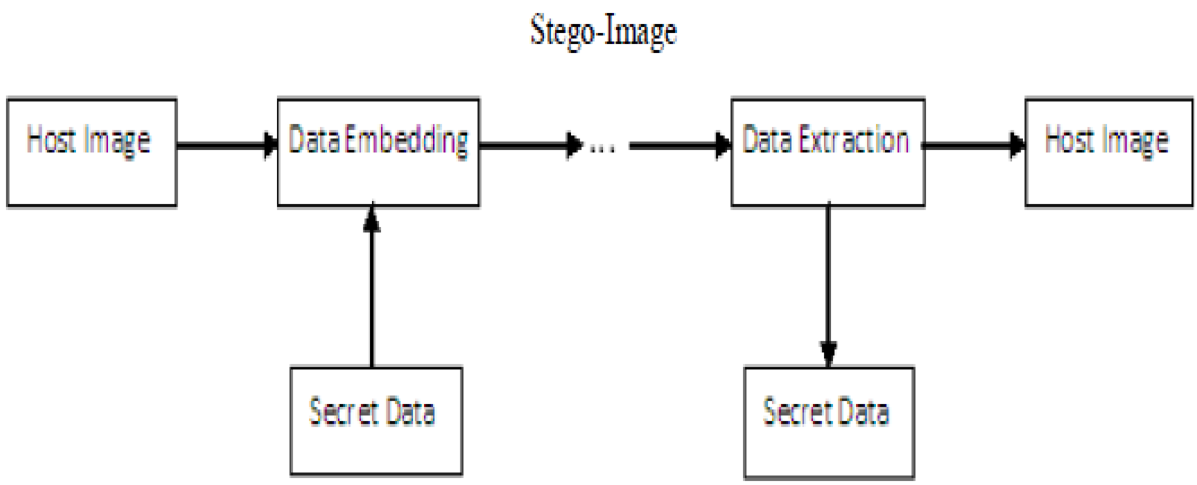

Fig.1. Data Hiding into Cover Image

- **Motivation**

Recently there are so many research is progressing on the field such as internet security, steganography, cryptography. This study describes the concept of data hiding technique which is established on steganography and internet security. When to send the confidential/important/secure data over an insecure and bandwidth-constrained channel it is habitual to encrypt as well as compress the cover data and then embed the confidential data into cover media.

For attaining this facility there are various encryption/decryption techniques, compression techniques, and data hiding techniques available. It is also important the data hiding should be reversible in nature while extracting, should be suitable for encryption/decryption domain.

Here we are analyzing the data hiding technique which is based on image feature extraction, image segmentation, attaching header information; blocks cluster formation and random pixel prediction by using the encrypted image as a cover data in which the data is embedded. Thus, it is termed as a watermarking or data hiding (DH) technique in image. Data hiding embeds information in a host media in a visually plausible way such that both the embedded message and the original host media can be exactly recovered.

Random Pixel Prediction (RPP) is an important technique of DH which can embed large payloads into digital images with low distortion and usually leads to a superior performance.

- **Need of proposed system**

As we discussed earlier, data hiding offers a way to embed data into host cover medium for the purposes of ownership protection, authentication, fingerprinting, secret communication and annotation in medical, military and law forensic area etc. In most data hiding algorithms, the cover data is destroyed permanently and cannot be exactly restored after the embedded message is extracted. Since there should be a need of such mechanism where both PEE and optimized histogram modification is used for getting optimized entropy by DH technique.

Data hiding by using PEE and OHM (optimized histogram modification) gives high prediction accuracy of pixels and high embedding capacity. DH ensures yours both host image and hidden data correct and extracted precisely.

The basic principle of this system is to reduce the distortion introduced by the DH by embedding data not only in to the current pixel of host image 'I' but also in to its prediction context.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

II.LITERATURE SURVEY

A considerable amount of research on reversible data hiding has been done over the past few years. The earliest reference to reversible data embedding we could find is the Barton patent [10], filed in 1994. In his invention, the bits to be overlay will be compressed and added to the bitstring, which will be embedded into the data block.

Honsinger, et al. [12], reconstruct the payload from an embedded image, and then subtract the payload from the embedded image to losslessly recover the original image. Macq [13] proposes an extension to the patchwork algorithm to achieve reversible data embedding. Fridrich, et al., develop a high capacity reversible data-embedding technique based on embedding message on bits in the status of group of pixels. They also describe two reversible data-embedding techniques for lossy image format JPEG.

De Vleeschouwer, et al. [13], propose a reversible data-embedding algorithm by circular interpretation of bijective transformations. Kalker, et al. [14], provide some theoretical capacity limits of lossless data compression based reversible data embedding and give a practical code construction. Celik, et al. [15] present a high capacity, low distortion reversible data-embedding algorithm by compressing quantization residues. They employ the lossless image compression algorithm CALIC, with quantized values as side-information, to efficiently compress quantization residues to obtain high embedding capacity.

Afterward more accuracy and more research have done in RDH techniques. Out of that we are focusing four important techniques are discussed here.

A. Integer Transform Technique

In this scheme, an integer transform is used to embed 1-bit watermark into one pixel pair in a way that the sum of the pixel pair remains unchanged. Based on the invariability of sum values and the equality between the parities of sum values and difference values, the extraction of watermarks and the recovery of pixel pairs can be easily achieved. Shaowei Weng et al.[16] proposed an integer transform in which the forward transform is defined.

B. Difference Expansion Technique

Yongjian Hu [17] uses the predicted image pixel error instead of the pixel-pair difference for Difference Expansion (DE) embedding. The recovery process also includes two manipulations. In the inner/embedded region, the embedded/hidden bit is extracted. In the shifted regions, the original pixel value is resumed. For difference expansion based reversible data hiding, the embedded bit-stream mainly consists of two parts: one part that conveys the secret message and the other part that contains the binary (overflow) location map and the header file.

C. Histogram Modification Technique

In histogram modification technique [18], the differences between adjacent pixels instead of simple pixel value is considered. Since image neighbor pixels are strongly correlated, the difference is expected to be very close to zero.

At the sending side, first scan the image in an inverse s-order and calculate the pixel difference d_i between pixels x_i-1 and x_i. These steps complete the data hiding and extraction process in which only one peak point is used. Large hiding capacities can be obtained by repeating the data hiding process. However, recipients may not be able to retrieve both the embedded message and the original host image without knowledge of the peak points of every hiding pass. To prevent overflow and underflow, histogram shifting technique is used that narrows the histogram from both sides.

D. Interpolation Technique

In this technique [19], the difference between interpolation value and corresponding pixel value is used to embed bit “1” or “0” by expanding it additively or leaving it unchanged. It is different from most differential expansion approaches in two important aspects:

1) It uses interpolation-error, instead of inter pixel difference or prediction- error, to embed data.
2) It expands difference, which is interpolation-error here, by addition instead of bit-shifting.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 3, Issue 11, November 2015

After secret messages are embedded, some overhead information is needed to extract the covert information and restore the original image.

E. Data Hiding Scheme Using Orthogonal Projection and Prediction Error Modification [20]:
The data hiding scheme is based on histogram shifting and prediction error modification. Orthogonal Projection Technique (OPT) is used for the optimal determination of the weights involved in a linear predictor. According to OPT, the value of the current pixel is predicted by a weighted sum of three of its previously visited neighbors.

All above discussed methodology having some lacunae like limited embedding capacity or less prediction capacity or recovered image quality is not good. Since we are trying to overcome all these lacunae in our developed system using random pixel prediction, image segmentation, block mapping and LSB.

III.SYSTEM IMPLEMENTATION

Our proposed system is mainly based on data hiding technique which is established on steganography and internet security. The data hiding process links two sets of data, a set of the embedded data in to host image and another set of the host image data. 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.

For this objective, we are dividing image into a block and hiding data into respective block by using block mapping algorithm, clustering algorithm and random pixel prediction algorithm to generate watermarked image.

Figure 2 shows architecture of data hiding (embedding) and Figure 2 shows architecture of data extraction.

System architecture

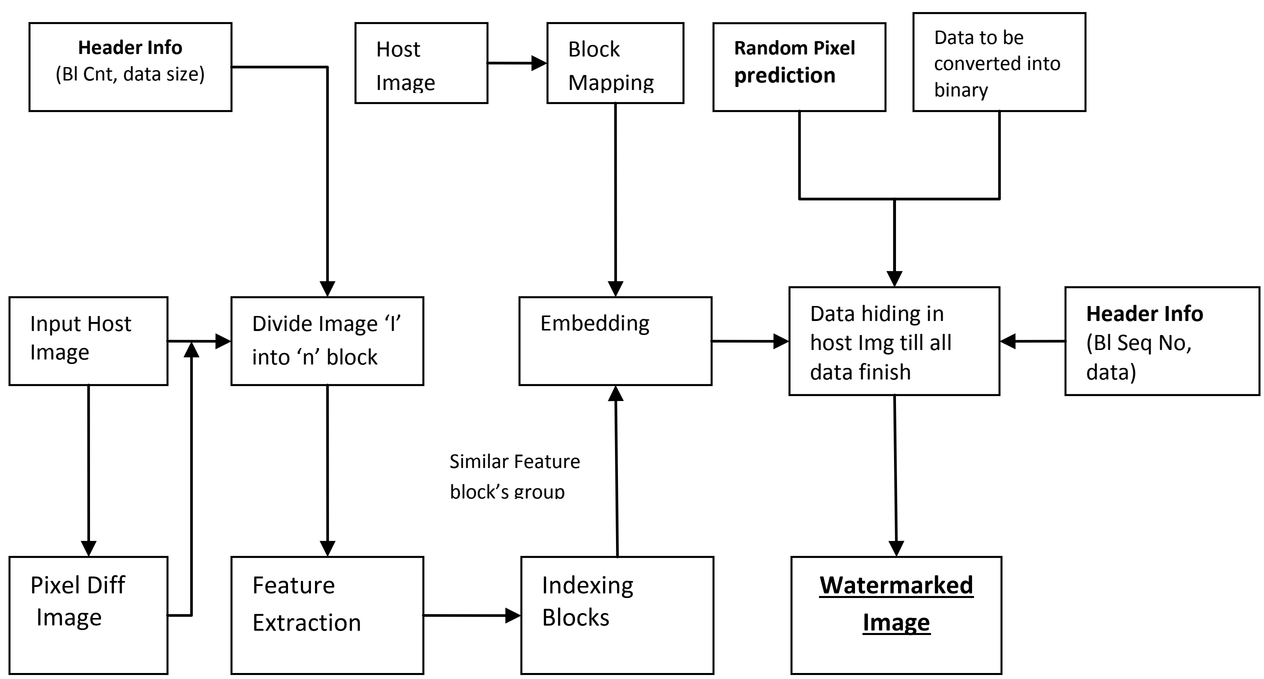

Fig 2: Architecture of data hiding (embedding)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

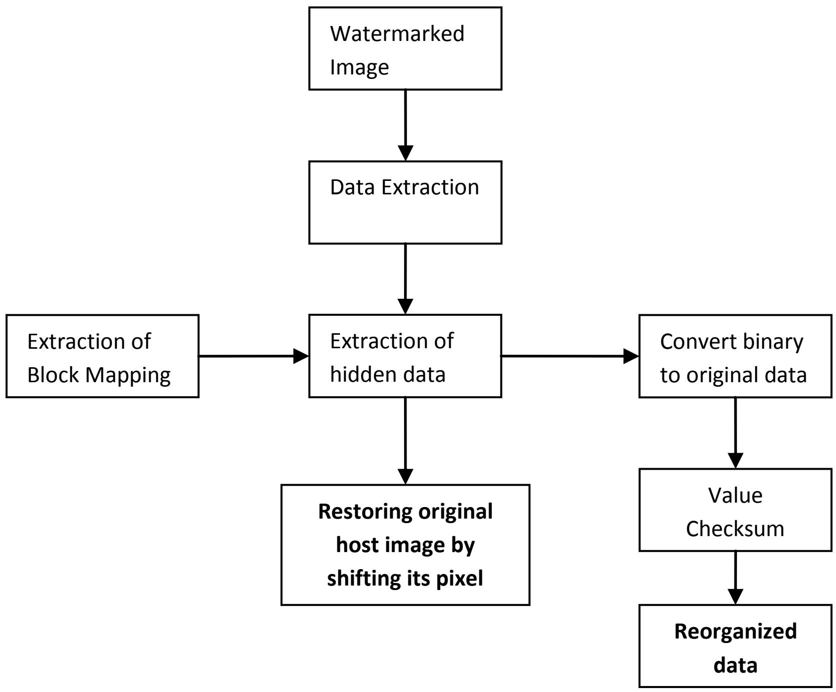

Fig 3: Architecture of data extraction

IV.METHODOLOGY

- **Data embedding:**

Identification of stego-bearing pixels, this technique uncovers the exact locations where the pixels are used to carry the message bits. Today's methods for the embedding of data into cover image divide into three categories: Least-Significant Bit, embedding transforms techniques, and methods that divide image into blocks.

A digital image consists of a matrix of color and intensity values. In a gray scale image there are 8 bits per pixel are used. In a full-color image there are 24 bits per pixel, and 8 bits assigned to each color components that means red, green and blue. The simplest steganographic techniques embed the bits of the message directly into the least-significant bit of the cover image in a deterministic sequence.

In Proposed system,

1. System takes input as a Host image and data which is to be hidden.
2. We are dividing host image into blocks of n*n formation. Then pixel difference is calculated for storing data and to locate exact position of pixel to store data.
3. Here data embedding is done after dividing the image into 'n' blocks. Then histogram of each block is plotted. After histogram modification, data is embedded into each block using the proposed embedding algorithm.
4. After dividing image into block, system adds header information to it (Bl cnt, data size).
5. Then block mapping to be done for getting exact location of stored data in host image at receiver side.
6. Indexing of block is done for storing data in sequence and identification of block at receiver side.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

7. Data is hidden in host image till all data finish. Hiding capacity is the size of data or information that can be hidden relative to the size of the particular cover. A huge hiding capacity allows the use of a smaller cover for a message of not variable size, so decreases the bandwidth required to transmit the stego-image.
8. Amount of information that can be embedded within image blocks are more as compared with embedding within a single image. This technique consists of three main stages. 1) Dividing the image into 'n' blocks 2) Processing stage 3) Embedding stage.
9. At the end again header information is added at each block. And finally watermarked image is created.
10. Secret data embedding and extraction can be performed with the same embedding and extraction algorithm. Same procedure is repeated for extracting data at receiver side where hidden data is extracted and it restored host image.

- **Data/Message extraction:**

Once the data has been embedded then it becomes available for further transmission or communication. When the transmitted data approaches to the receiver terminal then it is required to be extracted so that the text data being transmitted can be retrieved. The process of extracting the text data from the embedded or stego image is known as message extraction. This technique normally concerns with extracting and deciphering the hidden message to obtain a meaningful message.

V.CONCLUSION

This system propose a pixel prediction method for PEE based reversible data hiding schemes based on the minimum rate criterion, where our objective to maintain consistency between the two steps of PEE based reversible data hiding schemes i.e PEE and histogram modification.

Previously studied PEE models treat the two steps independently while they either focus on pixel prediction to obtain a sharp PE histogram, or aim at histogram modification to enhance the embedding performance for a given PE histogram. Therefore we are proposing a novel optimized histograms modification scheme which will achieve the optimal embedding performance.

REFERENCES

[1] M. Wu, H. Yu, and B. Liu, "Data hiding in image and video .II. designs and applications," IEEE Trans. Image Process., vol. 12, no. 6, pp. 696–705, Jun. 2003.
[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking Steganography, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.
[3] Shi Y. Q., Z. Ni, D. Zou, C. Liang, and G. Xuan, "Lossless data hiding: Fundamentals, algorithms and applications," in Proc. IEEE ISCAS, vol. 2. May 2004, pp. 33–36.
[4] Shi Y. Q., "Reversible data hiding," in Proc. IWDW, 2004.
[5] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," EURASIP J. Inf. Security, vol. 2010, Jan. 2010.
[6]Sunil Lee, Chang D. Yoo, "Reversible Image Watermarking Based on Integer to integer wavelet transform" 2007.
[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Vol. 13, No. 8, pp. 890–896, Aug.2003.
[8] ZhenfeiZhaoa, HaoLuoc,, Jeng ShyangPand, "Reversible data hiding based on multilevel histogram modification and sequential recovery" International Journal of Electronics and Communications, 2010.
[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding", IEEE Trans. Circuits Syst. Video Technol. vol. 16, no. 3, pp. 354–362, Mar. 2006
[10] J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5 646 997, 1997.
[11] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U.S. Patent 6 278 791, 2001.
[12] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in Proc. EUSIPCO, Sept. 2000, pp. 533–536.
[13] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Tran. Multimedia, vol. 5, pp. 97–105, Mar. 2003.
[14] T. Kalker and F. M. J. Willems, "Capacity bounds and constructions for reversible data hiding," in Proc. 14th Int. Conf. Digital Signal Processing, vol. 1, July 2002, pp. 71–76.
[15] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in Proc. Int. Conf. Image Processing, vol. II, Sept. 2002, pp. 157–160.
[16] Shaowei Weng, Yao Zhao, Jeng-Shyang Pan and Rongrong Ni,(2008), "Reversible Watermarking Based on Invariability and Adjustment on Pixel Pairs", IEEE signal processing letters, Vol. 15, pp. 721-724.
[17] Yongjian Hu, Heung-Kyu Lee and Jianwei Li,(2009), "DE- Based Reversible Data Hiding With Improved Overflow Location Map", IEEE Transaction on Circuits and systems for video technology, Vol. 19, No. 2, pp. 250-260.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

[18] Wei-Liang Tai, Chia-Ming Yeh and Chin-Chen Chang,(2009), "Reversible Data Hiding Based on Histogram Modification of Pixel Differences", IEEE Transaction on circuits and systems for video technology, Vol. 19, No. 6, pp. 906-910.

[19] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng and Zhang Xiong, (2010), "Reversible Image Watermarking Using Interpolation Technique " , IEEE Transaction on Information Forensics and Security, Vol. 5, No. 1, pp 187 – 193.

[20] W. Hong, T. S. Chen, Y. P. Chang and C. W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification", Signal Processing, vol. 90, (2008), pp. 35-46.

[21] Bo Ou, Xiaolong Li, Yao Zhao, Senior Member, IEEE, Rongrong Ni "Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DEC 2013.

[22] Xiaocheng Hu, Weiming Zhang, Xiaolong Li, and Nenghai Yu **"**Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding" IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.