Histogram Based Data Cryptographic Technique with High Level Security

Prof. Romi Morzelona

Professor, Department of Computer Science, IRU, Russia
romimorzelona@mail.ru

Article History	Abstract
	Histogram shifting plays a major role in reversible data hiding technique. By this shifting method the distortion is reduced and the embedding capacity may be increased. This proposed work uses, shifting and embedding function. The pixel elements of the original image are divided into two disjoint groups. The first group is used to carry the secret data and the second group adds some additional information which ensures the reversibility of data. The parameter such as PSNR, embedding capacity and bit rate are used for comparisons of various images ***Keywords:*** *Histogram, reversible elements, PSNR, Image processing*

I. Introduction

The image using in the data hiding method will be distorted permanently and not able to restore from the content which has been marked. Most applications in medical field which includes sharing of images multimedia management and the original image can't be recovered from distortion. To overcome this distortion, Reversible Data Hiding (RDH) method is developed and original image can be retrieved fully after the process of embedding. This method uses different techniques which ensure that original image gets recovered [1][2].

Host image gets divided into different pixel brace and the dissimilarity between the two pixel values is combining to a single bit. Up to 0.5 bits per pixel embedded rate can be achieved. Location map adopted by this algorithm is used to record he expandable locations [3]. The embedding rate can be increased upto 0.75 bits per pixel. Image redundancy is achieved using this algorithm and gives better performance when compared to the previous existing methods. Certain dimension of host image can be modified using histogram based RDH algorithm. Two major advantages will be highest modification of pixel standards can be inhibited and limiting the distortion values and the position map records the underflow & overflow location [4].

Data hiding is the process of hiding a data in a host image that is transmitting the data in a hidden manner. Hiding of a data in a host image is called as watermarked image. It is the secretly embedding data in graphics image and other types of files [5]. Data hiding method which covers the image to save image from attackers. Watermarking hides the information which is in digital form in a carrier signal. 90 percentage of water and 10 percentage of fiber are applicable for applying watermarking algorithm. In this high quality papers is made of a intended design [6].

Cryptography is a study of techniques of secure communication. There are encryption and decryption process. In encryption process the plain text is converted into cipher text. In decryption process the cipher text is divided into plain text [7]. Cryptography is the method of changing format of input at the transmitter side using encryption process and retrieving the original information at the receiver by decryption process. During transmission, no one can understand the original information and it is difficult to appreciate the information during transmission. Steganography is writing messages in a secured manner in which the sender and the receiver knows about the message. Hidden messages in such a way that only the sender and intended recipient. Different watermarking methods are:

a) Wire and Shaded watermarks
b) Random and localized watermarks
c) Reversible and irreversible watermarks
d) Visible and invisible watermarks
e) Blind and Non Blind watermarks
f) Semi-Fragile and Robust watermarking

Wire watermarks and Shaded watermarks: Design procedure involves fine wires soldered to the roll cover surface. Watermark pattern is designed by passing the stock under the dandy roll and it displays the fibre. Watermark appears lighter and for technical reasons heavier bond papers are used. Separate two rolls are used and the roll presses the paper being formed. In the depressed area fibres accumulates heavily and makes the surrounding area darker [8][9]. Two types of watermarks are employed and the first one random watermark then followed by localized watermark. The best way to produce watermark in a fashion in the sheet completed. Depends on the size, marks will be furnished to appear on a paper. In the sheet, random water mark will be appearing in any one of the location between top and bottom [10].

II. Related Works

Jing-ming Guo and Yun-fu Liu describes that Block Truncation Coding (BTC) is the best efficient compression method with less complexity[5].The two main deficiencies in this coding are blocking and false contour effects. The blocking and false contour effects are two major deficiencies in block truncation coding which cause severe perceptual artefacts. Error diffused BTC (EDBTC), improves blocking and false contour. Lingling and Dacheng Tao describe that reversible watermarking used in embedding watermarks [6]. The secret information is embedded into digital media.

Weiming Zhag, Giao Chen, Nenghai Yu describes that in Reversible Data Hiding (RDH), the image will be retrieved without any losses, once the information is extracted [8]. For RDH, a rate distortion model was established. Yhun-Hsien Chou and Kuo-Cheng Liu describe a way to satisfy the two requirements to embed high-strength watermark signals. This paper presents a colour image watermarking scheme.

Wei-Liang Tai, Chia-Ming Yehand Chin-Chen Chang depicted reversible information stowing away relying upon a histogram adjustment which incorporates the paired tree structure to take care of the issue. FPR strategy conveys the pinnacle point sets [9]. Pixel contrast circulation accomplishes the enormous concealing limit and makes the mutilation low. Yongijan Hu, Heung-Kyu Lee and Jianwei Li portrays that in Difference Expansion comprises of two sections. One section contains the mystery message and the other part contains implanting data. Hengfu Yang, Chang-TsunLi and Rong Xiao depict a plan which fulfills the applications where obvious watermark is utilized to battle copyright robbery [4].

III. Proposed Methodology

In proposed method, host image is divided into non overlapping blocks in which every block contains n number of pixels. The parameter 'a' is called the maximum occurrence of pixel values in an image, where the data is hidden in all the maximum occurrence of the pixel value in an image. The data is shifted and embedded according to the following conditions:

Step1: If x ∈ Ts (shifting function), the hidden data will not be carried by the block and value is will be shifted to g(x) ∈ An (image block) where x=An
Step2: If x ∈ Se (embedding function), a new pixel value is considered as fm(x) ∈ An where m∈ {0, 1} is the required data bit which is to be embedded.
Step3: If x ∈ Tu,o (underflow and overflow function) we know that g(x)∈ An. We do nothing with x to prevent underflow and overflow.
Step4: If x ∈ Su,o either f0(x)∈ An or f1(x)∈ An , block remains the same. The set up may be overlapped with g(Ts) f0(Se) f1(Se). Location map to record the locations of blocks.

The above procedure is made to carry the shifting and embedding functions. The two processes are
a) Data embedding
b) Data extraction

a. Data Embedding
Step1: Dividing an image into non- overlapping blocks
Step2: Define the location map
Step3: The blocks are divided into three groups. Three groups are used to carry underflow, overflow and embedded data. First and third group is to carry {0,255}.Second group carries the embedded information using shifting and embedded function.
Step 4: By the use of shifting and embedding functions, we can embed the hidden data into first and third group.
Step5: In the final step, embed the LSB sequence into second group the resultant image is called "marked image".

Here, the partitioning of three parts can able to solve the underflow/overflow problem. First group is double embedded to embed first the hidden data and   location map is embedded.

b. Data Extraction
Step 1: Similarly, image which is marked will be divided into non overlapping blocks.
Step 2: Determine location map by reading LSBs of first group.
Step 3: The blocks are divided into three groups.
Step 4: Extract the data from second group and the original pixel values can be recovered.
Step 5: Extract the embedded data from first and third group

Consider the following examples

44	111	44	90	12
100	45	22	68	44
30	27	44	23	98
44	171	255	45	57
226	45	0	9	45

Step1: Consider a input matrix 5*5
Step 2: The maximum occurrence is 45. The values less than maximum occurrence is decremented and greater than maximum occurrence is incremented.

45	111	45	90	12
99	45	22	68	45
31	27	45	23	98
45	171	255	45	57
226	45	0	9	45

Step 3: The data to be stored is 23. It is converted into binary, 23=00100011.

44	111	44	90	12
100	45	22	68	44
30	27	44	23	98
44	171	255	45	57
226	45	0	9	45

Step 4: The data is hidden into all maximum occurrence pixel value .The embedded pixel value is taken as 1 and remaining 0.

1	0	1	0	0
0	1	0	0	1
0	1	1	0	98
44	171	255	45	57
226	45	0	9	45

Step 5: At retrieving side, the embedded image is given as input. The presence of 1 is identified as embedded data. The LSB of embedded data is retrieved and output is obtained as23.

45	110	45	89	13
99	45	23	67	45
31	28	45	24	97
45	170	255	45	56
255	45	0	10	45

IV. Simulation Results and Discussions

Localized watermark is used for critical positioning. When the sheet is cut into letterhead size, the electronically controlled positioning system is used. This method centered in the lower region.

Reversible and Irreversible watermarking: The information can be fully retrieved using the first type and the information cannot be retrieved using the second method.

Visible and Invisible watermarking: The first type of watermarking are easily visible to eyes namely logos,etc. Without any type of calculation we can view the watermarks and one main disadvantage is that it can be destroyed easily. In the second type, the watermark can be viewed only to the authorized persons.This is more secure and more robust in nature.

Blind and Non-Blind watermarking: The schemes in which the cover signal information is not required during the detection process. During embedding process, random sequence is generated by a key. Such methods are known as blind watermarking. Detection process which requires the original information is known as non-blind watermarking.

Semi-Fragile and Robust watermarking: A semi-fragile watermark technique is of highly sensitive to a of the stego medium modification. The scheme can be able to detect the change in the signal and can able to identify the modification. The input image is shown in figure 1.
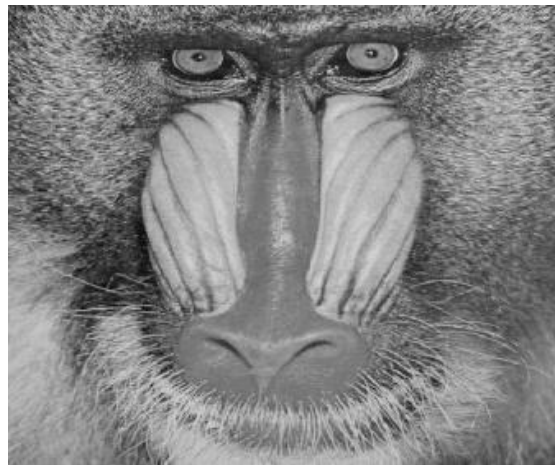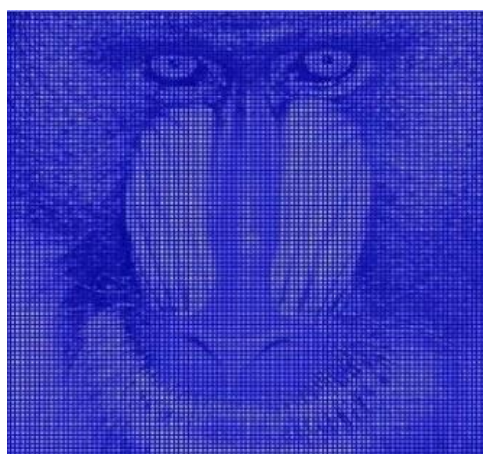

Fig 1: Input image

Fig 2: Dividing image into blocks

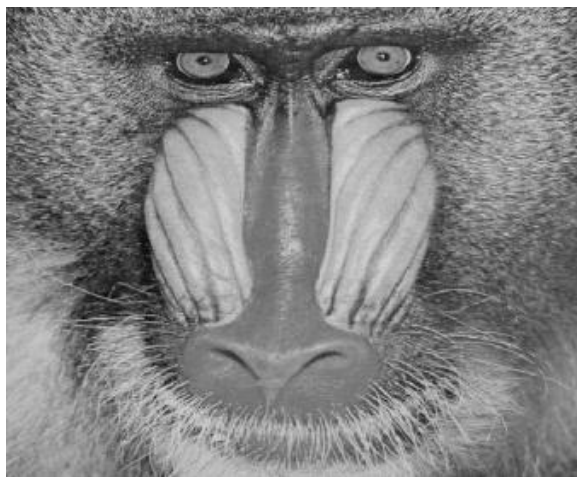The embedded data is13=00010011 and it o=is shown in figure 3.

Fig 3: Data embedded image

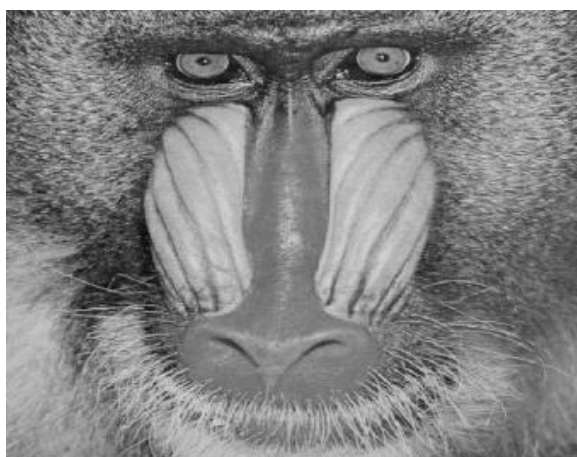The retrieved data is13=00010011 and is shown in figure 4.

Fig 4: Reconstructed image

The embedding rate is calculated for the above data embedded image. It ranges between 0.8 Bits Per pixel to 0.9 BPP. In existing work the embedding rate is obtained as 0.5. In our proposed work the reaches from 0.5 to 0.9 BPP. Hence the large amount of data can be hidden when compare to existing method. Thus the embedding rate is high, given input information is retrieved and the output image will be obtained without any distortion.

TABLE I PSNR and Embedding rate comparison for different images

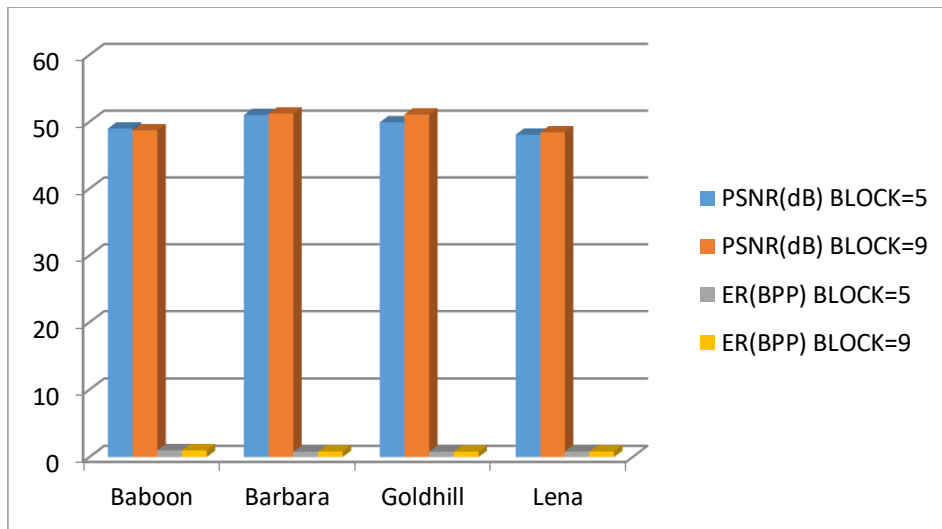| IMAGE	PSNR(dB)		ER(BPP)	
	BLOCK=5	BLOCK=9	BLOCK=5	BLOCK=9
Baboon	48.99	48.72	0.999	0.9999
Barbara	51.01	51.23	0.812	0.820
Goldhill	49.92	51.09	0.809	0.806
Lena	48.06	48.42	0.814	0.815

Fig 5: Comparison of various secured image parameters

V. Conclusion

In this paper, HS- based RDH method is proposed. In this by defining embedding and sifting functions, we can obtain RDH algorithm. This work explains the design of RDH. These algorithms give better performance and high embedding rate(ER). The PSNR for the input image and reconstructed image is 45.3.The same process will be done in colour image in future work.

References

[1] Gouenou Coatrieux, Clara Le Guillou, Jean-Michel Cauvin and Christian Roux (March 2009) "Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images", IEEE transactions on Information Technology in Biomedicine, vol. 13, No. 2,pp.880-886.

[2] Hengfu Yang, Chang-Tsun Li and Rong Xiao (December2009) "A Contrast- Sensitive Reversible Visible Image Watermarking Technique", IEEE transaction on Circuits and Systems for Video Technology, vol.19, No.5.pp 638-648.

[3] L. Zhao and Y. Wan, "An Edge-Guided Exact Histogram Specification Method for Enhancing Extremely Dark Images," 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), Dalian, China, 2017, pp. 612-616, doi: 10.1109/ICCTEC.2017.00138.

[4] Jing-Ming Guo and Yun-Fu Liu(May 2012), "High capacity data hiding for error- diffused block truncation coding", IEEE transaction on Image Processing, vol.21, No.12,pp.187-193.

[5] LinglingAn and Dacheng Tao (June2012) "Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking", IEEE transaction on Image Processing, vol.21, No.8,pp.826-832.

[6] Srdjan Stankovic, Irena Orovic and Nikola Zaric (2010) "An Application of Multidimensional Time-Frequency Analysis as a Base for the Unified Watermarking Approach", IEEE transaction on Image Processing, vol.19, No.3,pp.255-258

[7] WeimingZhag, Giao Chen, Nenghai Yu (December 2012), "Reversible Watermarking Algorithm Using Sorting and Prediction", IEEE transaction on Circuits and Systems for Video Technology, vol.19, No.7,pp.234-230.

[8] Wei-Liang Tai, Chia-Ming Yeh and Chin- Chen Chang (March2009) "Reversible Data Hiding Based on Histogram Modification of Pixel Differences", IEEE transaction on Circuits and Systems for Video Technology, vol.19, No.6,pp.474-484.

[9] Young-Yoon Lee, Sang-Uk Park, and Chang-Su Kim (June2009) "Temporal Feature Modulation for Video Watermarking", IEEE transaction on Circuits and Systems for Video Technology,vol.19, No.4,pp.906-910.