Reversible Watermarking based on Entropy Masking with Histogram Shifting

Rashpinder Kaur
Department of Computer Science & Engineering
CU, Mohali
Student at Chandigarh University

Jaspreet Singh
Department of Computer Science & Engineering
CU, Mohali
Assistant Professor at Chandigarh University

ABSTRACT
In this paper an improved method for reversible watermarking is proposed. This scheme is the combination of entropy masking and histogram. One first contribution is entropy masking which has three techniques. From three of them dwt is used for the watermarking. Entropy masking is also a human visual system's characteristic, which rarely has been addressed in visual models. The second contribution is a histogram shifting. This will show the histogram of the different images. In that way the watermark embedded and extractor remain synchronized for message extraction and image reconstruction. In this paper a universal entropy masking model is proposed for watermarking embedding algorithm to keep the balance between watermarks' imperceptibility and also its robustness. Also the results are concluded from the experiments that a suitable domain of entropy calculation will result in optimal watermarking performance. For the implementation of this proposed work, the Matlab software is used under image processing toolbox.

Keywords: Digital Watermarking, Entropy, Entropy Masking, Histogram Shifting, PSNR (peak signal to noise ratio)**.**

1. INTRODUCTION
Digital watermarking is a process in which some information is embedded within a digital media so that the inserted data becomes part of the media [8]. This technique has several numbers of applications such as broadcast monitoring, data authentication, data indexing and so on. A digital watermarking system must successfully satisfy trade-offs between conflicting requirements of perceptual transparency, data capacity and robustness against attacks. Watermarks have two categories of roles: In the first category, the watermark is considered as a transmission code and the decoder must recover the whole transmitted information correctly. In the second category, the watermark serves as a verification code. In the latter system, the watermark detector must simply determine the presence of a specific pattern. In two decades a vast demand for digital media transmission and distribution has made the copyright protection of multimedia contents to be a great concern. Since encryption system became an approach of content protection in communications, the development of digital watermarking technology has made it possible once those contents are decrypted. The most important performances of a digital watermarking system are imperceptibility and robustness [8] [20].

Since the introduction of the concept of reversible watermarking, several methods have been proposed. Except these solutions, most recent schemes used are Expansion

Embedding modulation, Histogram Shifting modulation. One of the main concerns with these modulations is to avoid underflows and overflows. The precaution must be taken to avoid gray level value underflows (-ve) and overflows (+) (greater than for a bit depth image) in the watermarked image when the watermark signal is added to the image while minimizing at the same time image distortion. As analysed above, the large entropy area is good for watermarking embedding and that is the true hidden channel. In general, entropy masking in watermarking system experiences three steps. Over recent years, there has been tremendous effort in order to understand and model the Human Visual System and applying it to different image processing applications. Such effort has been examined for solving various problems and has resulted in different levels of success.

Introduced the well-known Histogram Shifting (HS) modulation [19] [21]. HS adds gray values to some pixels in order to shift a range of classes of the image histogram and to create a 'gap' near the histogram maxima. The pixels are shifted to the gap or kept unchanged to encode one bit of the message '0' or '1' which belong to the class of the histogram maxima ("*Carrier-class*"). Other pixels (the "non-carriers") are simply shifted. To avoid working in the spatial domain, many schemes apply HS to some transformed coefficients [15] or pixel prediction-errors, histograms of which are most of the time concentrated around one single class maxima located on zero. This maximizes HS capacity [17] and also simplifies the re-identification of the histogram classes of maximum cardinality at the extraction stage. In order to reduce the distortion in the images while preserving the embedding capacity, to identify pixels, transformed coefficients or prediction-errors that belong to the histogram minima classes, some preprocessing techniques has been suggested in order. As we will see later, different schemes working with prediction-errors do not watermark pixels within a neighborhood of high variance [9]; indeed, these pixels belong to histogram classes that are shifted without message embedding.

2. REVERSIBLE WATERMARKING
Watermarking is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal [5]. Watermarking has been further divided into two types: perceptible watermarking and imperceptible watermarking. Perceptible watermarks are visible in nature and they shows to human eye. This type of watermark can be a logo, name etc. on the other hand, imperceptible watermark are visible in nature. The watermark is hidden behind some data. If someone wants to see them, user should have to extract them with using of specific algorithms. This type of watermark can

be audio signal, image, text document etc. the watermarking is used for the purpose of authentication/ownership so that no other person says that data to his own. Traditional watermarking used visible watermarks which can be easily removed from the picture by cropping or editing. But nowadays invisible watermarking is used. In this technique a digital signal is added as a watermark to the data which is hidden. The digital signal may be audio, video, image, text, 3D models. The invisible watermarking is also known as digital watermarking.

Digital watermarking [10] is one of the proposed solutions for copyright protection of multimedia data. This provides more security than the other schemes. So this technique is better than Digital Signatures and other methods because it does not increase overhead. In this paper here is presenting a new image watermarking technique that can embed more number of watermark bits in the cover image without affecting the imperceptibility and increase the security of watermarks as well as quality of image. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The digital signal may be image, text, audio, pictures or video. In this paper input image is act as a host signal and embedding the secret data in it and the extract the same. In this process we can enhance the network security.

Reversible watermarking [7][18]is data hiding technique that embeds secret information into a host media without loss of host information. These methods allow the user to restore exactly the original image from its watermarked version by removing the watermark from the image. Reversible data hiding method based on histogram shifting which can recover the original image lossless after the hidden data has been extracted from the stego-image. The method of prediction is adopted in our proposed scheme and prediction errors are produced to explore the similarity of neighbouring pixels. Thus it becomes possible to update the watermark content. In this the original image can be recovered from the watermarked image without any degradation/distortion from the watermarked image after extracting the secret message embedded.

3. HISTOGRAM SHIFTING

Histogram shifting [4] (HS) is a useful technique of reversible data hiding (RDH). With HS-based RDH, high capacity and low distortion can be achieved efficiently. The HS technique and present a general framework to construct HS-based RDH. With the proposed framework, one can get a Histogram shifting algorithm by simply designing the so-called shifting and embedding functions. By taking this specific shifting and embedding functions, we show that several HS algorithms reported in the literature are special cases of this general construction. It is expected that more efficient HS algorithms can be devised according to the proposed framework by carefully designing the shifting and embedding functions.

The histogram shifting involves calculation of the prediction errors to generate a difference image from the correlation of the neighbourhood pixels and then embedding the secret bits in the prediction errors. Here, we cannot predict the complete image at one go as in traditional prediction technique. So an image is divided into non-overlapping blocks and then uses the prediction technique to generate the prediction error blocks or to generate the prediction error. From gray-value distribution in an image, we observed the characteristics of an image carefully and found out that the pixel values are highly correlated among each other. The prediction, we have to leave some pixels unused for successful reconstruction. We propose

to use prediction errors to apply the histogram shifting algorithm. The reasoning behind this is that the histogram shifting algorithm uses the peak point to embed the secret information into the algorithm. We are going to embed the type of data based on the application we are using. In the Odd-Even histogram shifting first we are going to consider the Odd columns and then the Even columns were we are going to find the Highest peak points for data insertion. First the secret image is hidden inside the cover image and in the highest peak point the data has been embedded for watermarking. In this type of data insertion the Payload will be high while comparing to the previous systems.

Following are the Steps used for histogram shifting in the proposed system:-

Insertion:-

Step1. Find image histogram.

Step2. Shift histogram with fixed magnitude.

Step3. Message or data is converted in the form of 0 and 1.

Step4. Insert our converted data in this gap.

Step5. Then again shift histogram.

Extraction:-

Step1.We will shift back shifted value and extract our data.

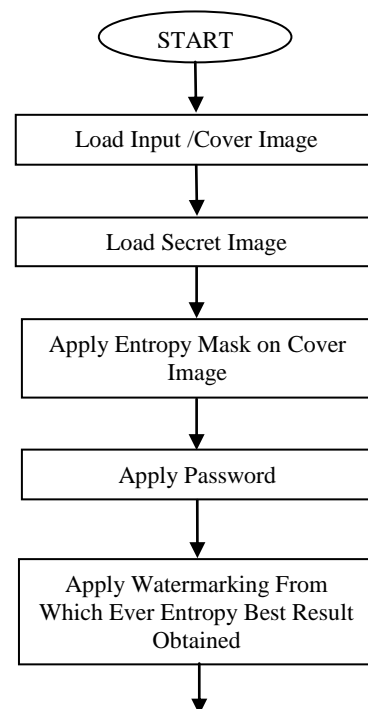Step2. Convert back to message from 0 and 1 form.
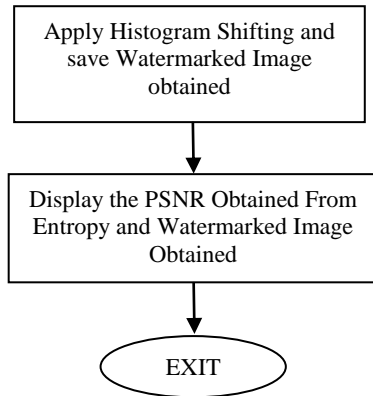
4. ENTROPY

Entropy [11] is a statistical measure of randomness that can be used to characterize the texture of the input image.

Let P contains the histogram counts. The entropy is represented as

$$E = -\sum p \, log_2(P) \qquad (1)$$

5. PROPOSED METHODOLOGY

```
        ┌─────────────┐
        │    START    │
        └──────┬──────┘
               ↓
   ┌───────────────────────┐
   │ Load Input /Cover Image│
   └───────────┬───────────┘
               ↓
   ┌───────────────────────┐
   │   Load Secret Image    │
   └───────────┬───────────┘
               ↓
   ┌───────────────────────┐
   │ Apply Entropy Mask on  │
   │      Cover Image       │
   └───────────┬───────────┘
               ↓
   ┌───────────────────────┐
   │    Apply Password      │
   └───────────┬───────────┘
               ↓
   ┌───────────────────────┐
   │ Apply Watermarking From│
   │ Which Ever Entropy Best│
   │    Result Obtained     │
   └───────────┬───────────┘
               ↓
```
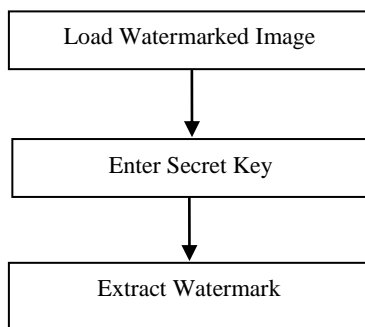
Fig.1. Steps carried out for the watermarking process in the proposed system

The figure shown as above is the flow diagram of embedding the watermark to an image with the use of entropy masking and histogram shifting. At from starting, we can read two different images which are of grey level images. First image is taken as a host image and the second one is taken as digital watermark. After that entropy masking is applied on the host image to show the image in different domains. Then a secret key is generated for the security purpose. This key is helpful in extracting the watermark. The watermark is applied using dwt technique under entropy masking and histogram shifting. The watermarked image is created and shown. Then the different PSNR values of different domains as well as watermarked image are calculated and results of PSNR are shown. Then the embedding capacity of watermark in the image is calculated. More is PSNR value as well as embedding capacity; better quality of image is produced. It the fact to shows quality of an image after embedding watermark to an image.

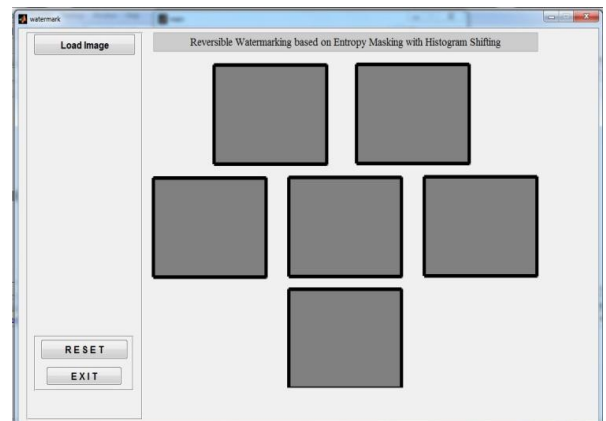The following chart shows the steps carried out in de watermarking process.

Fig.2. Steps carried out for the de-watermarking process in the proposed system
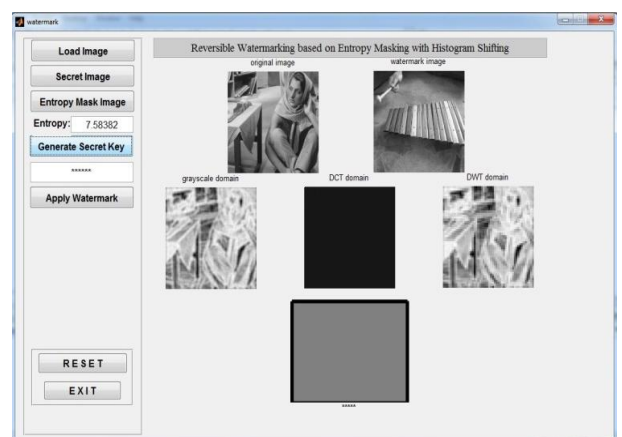
6. EXPERIMENT RESULTS

The following are the results obtained from the proposed system:-

Fig.3: The basic layout of the proposed system

Fig.4: The image is loaded

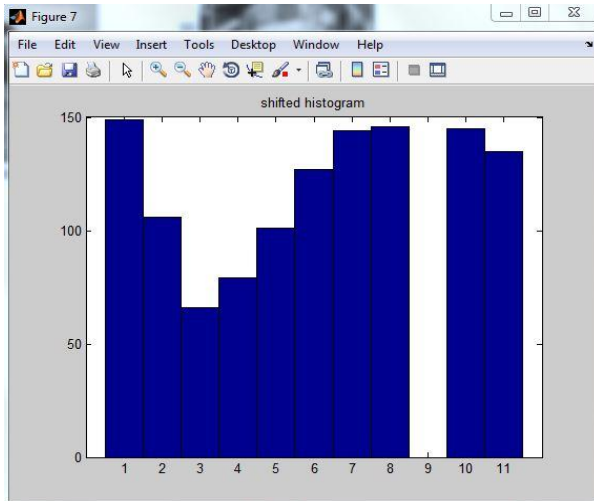**Fig.5: The entropy and the secret key are generated**
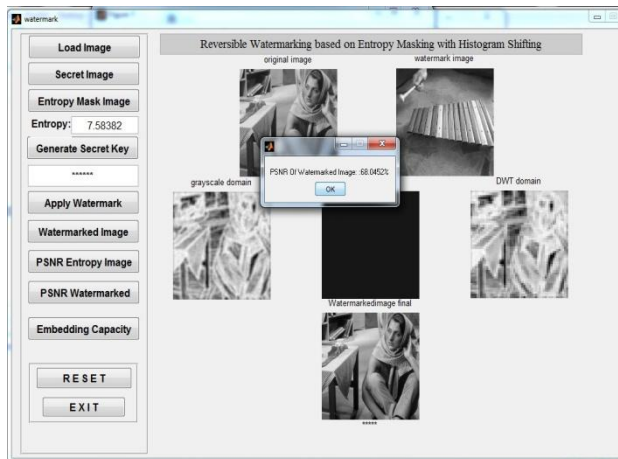
Fig.6: The Histogram Shifting is been plotted

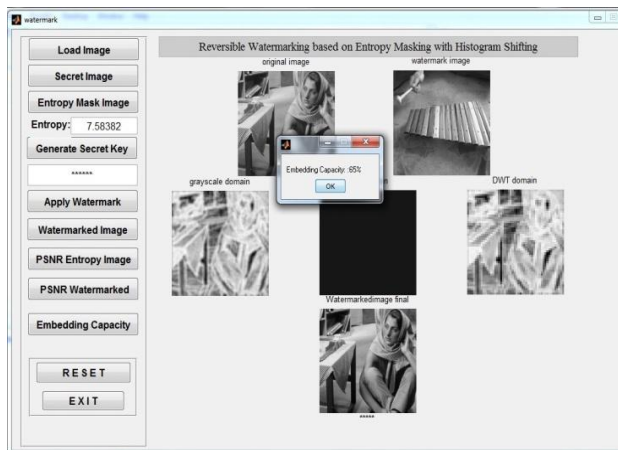

Fig.7: Calculate PSNR

Fig.8: Calculate Embedding Capacity

Fig.9: The De-watermarking layout

The table shows different PSNR value and embedding capacity of watermarked images. The table is as shown below:

Table 1: Table with different values of PSNR & EC

Sr. No	Name of combined images	PSNR (%) of Watermarked image	Embedding capacity (%) of an image
1	Camera.bmp and girl.png	68.8978	64
2	Girl.bmp and lena.jpg	68.0452	65
3	Monkey.bmp and camera.bmp	59.316	69
4	Bridge.png and monkey.bmp	60.862	67
5	Lena.jpeg and bridge.png	69.834	65

Formulas used:

1. $\quad$ PSNR $= 10 \log_{10} \dfrac{MSE}{(255)^2}$

2. $\quad$ MSE $= \dfrac{e}{m*n}$

   Where e= e+double [image1 (i,j)-image2 (i,j)]² a,

   Initial e=0

3. $\quad$ Embedding Capacity $= \dfrac{2E-A}{2A}$ bpp

   Where A= Total number of pairs
   $\quad$ E= Pairs with embedding information
   2E-A= Final space for embedding watermark in bits

7. CONCLUSIONS

In this paper, a new reversible watermarking scheme is proposed which originality stands in identifying parts of the image that are watermarked using two distinct HS modulations: Pixel Histogram Shifting and Dynamic Prediction Error Histogram Shifting. In this paper the essence of information transmission in digital watermarking system is also discussed and the dissymmetric digital watermarking framework lived on media content communication. Then a universal entropy masking model is proposed for watermarking embedding algorithm to keep the balance between watermarks' imperceptibility and its robustness. The concluded results which are calculated from the different experiments have a suitable domain of entropy calculation that results in optimal watermarking performance.

8. REFERENCES

[1] Gouenou Coatrieux, Wei Pan, Nora Cuppens-Boulahia. "Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting", IEEE transactions on information forensics and security, vol. 8, no. 1, Jan 2013.

[2] Youngseok Lee and Jongweon Kim. "Histogram Rotation-Based Image Watermarking with Reversibility ," International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

[3] Rakesh Ahuja S.S. Bedi Himanshu Agarwal, "A Survey of Digital Watermarking Scheme", MIT International Journal of Computer Science & Information Technology, vol. 2, issue 1, pp. 52-59, Jan. 2012.

[4] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011.

[5] W. Pan, G. Coatrieux, N. Cuppens, F. Cuppens, and C. Roux, "An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform," in Proc. IEEE EMBC Conf., Buenos Aires, Argentina, 2010, pp. 4740–4743.

[6] H. J. Hwang, H. J. Kim, V. Sachnev, and S. H. Joo, "Reversible watermarking method using optimal histogram pair shifting based on prediction and sorting," KSII, Trans. Internet Inform. Syst., vol. 4, no. 4, pp. 655–670, Aug. 2010.

[7] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[8] M.A. Akhaee and Bulent Sankur, "Robust Scaling-Based Image Watermarking Using Maximum-Likelihood Decoder With Optimum Strength Factor", IEEE Trans. on multimedia, vol. 11, no. 5, Aug. 2009.

[9] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 158–165, Mar. 2009.

[10] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuit Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[11] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognition., vol. 41, pp. 3582–3591, 2008.

[12] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636 © 2007 Science Publications.

[13] D.M. Thodi and J. J. Rodriquez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.

[14] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A review of image watermarking applications in healthcare," in Proc. IEEE EMBC Conf., New York, 2006, pp. 4691–4694.

[15] Z. Ni, Y. Q. Shi, N. Ansari, and S.Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[16] F. Bao, R. H. Deng, B. C. Ooi, andY. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. Inf. Technol. Biomed., vol. 9, no. 4, pp. 554–563, Dec. 2005.

[17] G. Xuan, Y. Q. Shi, C. Y .Yang, Y. Z. Zheng, D. K.Zou, and P. Q. Chai, "Lossless data hiding using integer wavelet transform and threshold embedding technique," in Proc. Int. Conf. Multimedia and Expo, 2005, pp. 1520–1523.

[18] L. Kamstra and H. J. A. M. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," IEEE, Image Process., vol. 14, no. 12, pp. 2082–2090, Dec. 2005.

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

[20] H. M. Chao, C. M. Hsu, and S. G. Miaou, "A data-hidding technique with authentication, integration, and confidentiality for electronic patient records," IEEE Trans. Inf. Technol. Biomed., vol. 6, no. 1, pp. 46–53, Mar. 2002.

[21] J. M. Barton , "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5 646 997, 1997.