IJETST- Vol.||02||Issue||05||Pages 2499-2506||May||ISSN 2348-9480 2015

Open access Journal International Journal of Emerging Trends in Science and Technology

Securing Digital images using Reversible Watermarking by Pixel Histogram Shifting

Authors

Kirti P. Sahare[1], Prof. S. A. Murab[2], Prof.G.M.Ghonge[3], Prof.M.V.Sarode[4]

Department of Computer Engineering, Sant Gadge Baba University, Amravati

Email: *kitisahare4u@rediffmail.com[1], sachinmurab21@gmail.com[2],mangesh.cse@gmail.com[3]*
mvsarode2013@gmail.com[4]

Abstract

A new reversible watermarking Scheme is proposed .One first contribution is a histogram shifting modulation which adaptively takes care of the local specificities of the image content. By applying it to the image prediction-errors and by considering their immediate neighbourhood, the scheme proposed inserts data in textured areas where other methods fail to do so. Furthermore, this proposed scheme will use a classification process for identifying parts of the image that can be watermarked with the most suited reversible modulation. This classification is based on a reference image derived from the image itself, a prediction of it, which has the property of being invariant to the watermark insertion. In this way, the watermark embedder and extractor will remain synchronized for message extraction and image reconstruction. The proposed scheme will improve a peak signal to noise ratio (PSNR) as compared to other existing scheme.

Keywords: *watermarking, PSNR, histogram*

1. Introduction

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "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. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.Several reversible watermarking schemes have been proposed for protecting images of sensitive content, like medical or military images, for which any modification may impact their interpretation. These methods allow the user to restore exactly the original image from its watermarked version by removing the watermark. Thus it becomes possible to update the watermark content, as for example security attributes (e.g., one digital signature or some authenticity codes), at any time without adding new image distortions. However, if the reversibility property relaxes constraints of invisibility, it may also introduce discontinuity in data protection. In fact, the image is not protected once the watermark is removed. So, even though watermark removal is possible, its imperceptibility has to be guaranteed as most applications have a high interest in keeping the watermark in the image as long as possible, taking advantage of the continuous protection watermarking offers in the storage, transmission and also processing of the information . This is the reason why, there is still a need for reversible techniques that introduce the lowest distortion possible with high embedding capacity. A new reversible watermarking scheme is proposed which originality stands in identifying parts of the image that are watermarked using distinct HS modulations: Pixel Histogram Shifting and visual cryptography.

2. Literature Review & Related work

Proposed a new way to share and enhance medical image functionalities. While watermarking allows the sharing of information independently from the image format, the proposed knowledge digest gives a synthetic description of the image content, a digest that can be used for retrieving similar images with either the same findings or differential diagnoses. KD combined with watermarking appears to be a flexible solution to provide updates for distant user similarity rules, and case and knowledge databases. [1]

Focuses on the complementary role of watermarking with respect to medical information security (integrity, authenticity) and management. Reviewed sample cases where watermarking has been deployed. Concluded that watermarking has found a niche role in healthcare systems, as an instrument for protection of medical information, for secure sharing and handling of medical images. [2]

This paper presented a simple and efficient reversible data-embedding method for digital images. Explored the redundancy in the digital content to achieve reversibility. Both the payload capacity limit and the visual quality of embedded images are among the best in the literature. [3]

Proposed a novel robust lossless image data hiding scheme, which employs a robust statistical quantity to mitigate the effect of image compression and small incidental alteration for data embedding. [4]

This Paper presented the histogram-shifting technique to remedy the two major drawbacks of Tian's algorithm: the lack of capacity control and undesirable distortion at low embedding capacities. This then described two new reversible watermarking algorithms, combining histogram shifting and difference expansion: the first one using a highly compressible overflow map and the second one using flag bits. A new, reversible, data-embedding technique called prediction-error expansion was then introduced and watermarking algorithms based on the prediction- error expansion technique were presented. [5]

Here the proposed reversible watermarking algorithm is a combination of efficient well-known existing techniques and new techniques which enables performance significantly. Using a new rhombus prediction scheme enables the efficient exploitation of sorting. A set of sorted prediction errors can be efficiently used for low distortion data hiding. The histogram shift method exploited over the sorted prediction errors produces excellent ratio between capacity and distortion. [7]

3. Proposed Work

The scheme relies on "invariant" classification process for the purpose of identifying different sets of image regions. These regions are then independently watermarked taking advantage of the most appropriate HS modulation. It distinguishing two regions where HS is directly applied to the pixels or applied dynamically to pixel prediction-errors respectively. The modulation is referred as PHS (for "Pixel Histogram Shifting") or DPHS (Dynamic Pixel Histogram Shifting.The choice is based on image data set, for which PHS may be more efficient and simple. [20]

In this proposed work, first of all we will take a source image then divide into number of equal parts. Then apply pixel histogram shifting algorithm to add watermark to each image. In HS modulation embedder classify one part of the message is embedded in PPHS region and another is in DPEHS region. Then plot the graph of every part of the image i.e. bar char. In the pixel histogram pixel value at x-axis and count on y-axis. After applying watermark then we will merge the image into one and apply *visual cryptography. In visual Cryptography* the method will divide the images into n number of shares and then add that shares into envelope to transfer by encryption. At the decryption level the original image is retrieved by using LSB Retrieval method. In this way we will get an original image. Let us go with the flow chart to understand the process:

4. Methodology

4.1 Reversible Watermarking Techniques

Several methods have been proposed for watermarking, among these solutions. Here we are using Dynamic Pixel Histogram Shifting and

Pixel Histogram Shifting modulation. One of the main concerns is to avoid underflows and underflows. Basically in DPHS, the highly textured part which contains non-carriers has to be shift in such region so as to add watermark. In this technique the watermark embedder and extractor remain synchronized with each other so as to manage the threshold value. Well known Histogram Shifting (HS) modulation. HS adds gray values to some pixel sin order to shift arrange of classes of the image histogram and to create a ’gap’ near the histogram maxima. Pixels which belong to the class of the histogram maxima (“*Carrier-class*”) are then shifted to the gap or kept unchanged to encode one bit of the message ’0’ or ’1’. Other pixels (the “no carriers”) are simply shifted. Instead of working in the spatial domain, several schemes apply HS to some transformed coefficients [10]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 and also simplifies there- identification of the histogram classes of maximum cardinality at the extraction stage.

4.2 Pixel Histogram shifting Algorithm:

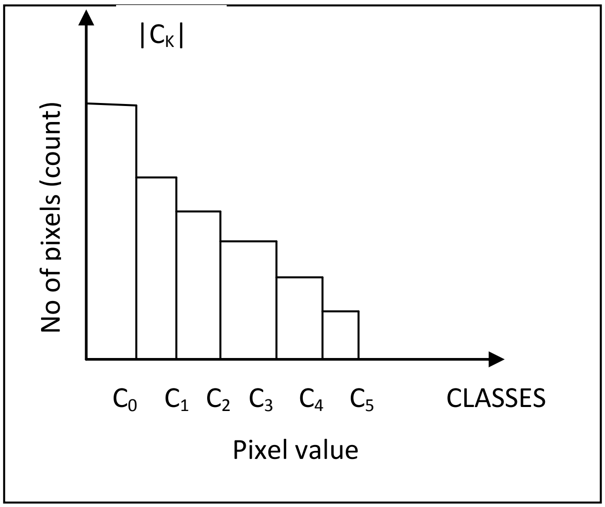
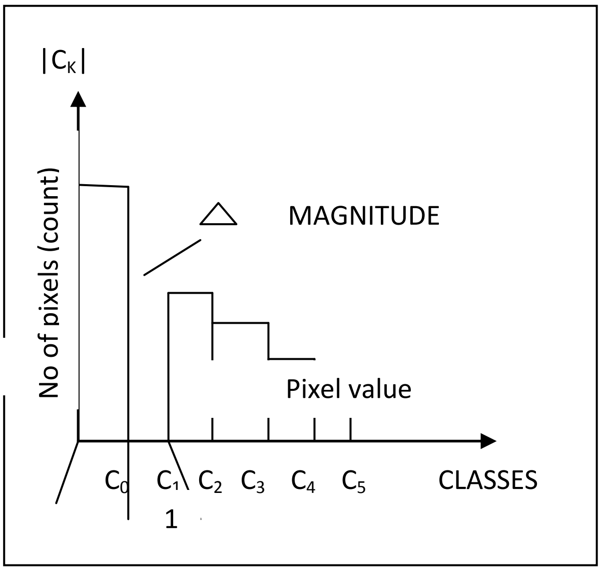


Fig2.Histogram shifting(a) original histogram



(b) Histogram of watermarked data

The basic principle of Histogram Shifting modulation, illustrated in Fig.1 in a general case, consists of shifting arrange of the histogram with a fixed magnitude Δ,in order to create a 'gap' near the histogram maxima(C_1in Fig.1) . Pixels, or more generally samples with values associated to the class of the histogram maxima (C_0 in Fig.1(b)),are then shifted to the gap or kept unchanged to encode one bit of the message ,i.e., '0' or '1' . As\stated previously, we name samples that belong to this class as "*carriers*". Other samples i.e.,"*no carriers*", are simply shifted. At the extraction stage, the extractor just has to interpret the message from the sample so the classes C_0 and C_1 and invert watermark distortions (i.e. shifting back shifted value).Obviously, in order to restore exactly the original data, the watermark extract or needs to be informed of the positions of samples that have been shifted out of the dynamic range. This requires the embedding of an overhead and reduces the watermark capacity.Typically this overhead corresponds to alocation map(avector)whose components in forms the extractor if samples of value are original values or shifted values. In fact, considering the example in Fig.1, the HS payload (C), i.e., the number of message bits embedded per sample of host data, is defined as: Where C_0 is the class of carrier samples (seeFig.1), and C_{VMAX} is classes associated to "overflows" and | |gives the class cardinality.

In Dynamic Prediction Error Pixel Histogram Shifting, the prediction error is considered while shifting and adding watermarked to it. Invariant classification is done to indentify which region is watermark able. The objective is to differentiate the watermark able pixel from others by invariant classification. So this is to be done before applying DPEHS. By this extractor will know which pixel is to be watermarked. Thus after having watermarked a pixel, embedder checks for an underflow and overflow from the extractor point of view and if it changes the threshold values.

The above algorithm is described as steps in the following manner:

Step 1: First of all take the source image that you want to watermarked

Step2: Divide the image into quarters so as to shift the carrier pixel

Step3: Thenin HS modulation pixels are divided into parts one is to PHS and other is to DPEHS depending on the invariant image classification and prediction-error. And graph should go beyond range that's why we decide threshold value i.e. $T_{min}$and $T_{max,}$ to manage underflow and overflow.

Step3: Then plot a histogram of the image as count of values v/s image intensity (0 to 255) that is on x-axis color value and on y-axis no of pixels of that color in the image. And this will be the bar chart and every bar represents the intensity level that is how many pixels have corresponding color.

Step4: Then after plotting histogram shift the carrier sample by a fixed magnitude so as to watermark the pixel.

Step5: Repeat the step3 and step4 for all the quarter part of the image so as to plot histogram.

Step6: After plotting and watermarking merge the quarters so as to get the original image with watermark.

Step7: Now we can apply visual cryptography to transfer the image with security.

4.3.Introduction to visual cryptography:

Visual Cryptography is a new Cryptography technique which is used to secure the images. In Visual Cryptography the image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the bi-level or binary images or monochrome images. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms.

5. Overall Scheme:

Algorithm used for scheme:

To sum up, this algorithm runs through the image between one and four times. Each embedding pass is conducted independently from the other on one quarter of the image pixels considering the following procedure. The stepwise algorithm is:

1. Considering a specific run into the image possibly based on a secret key.
2. One part of the message is embedded in the PHS region with some overhead in case of overflows/underflows.
3. Rest of the message is:

A. The classification thresholds T_{min} and T_{max} are computed in others. At the same time the embedder verifies if the extractor will find or not the same thresholds.

B. The message embedding is conducted in one or two stages depending on T_{min} and T_{max}.

In the following experiments, the embedded message is a binary sequence randomly generated according to a uniform distribution.

At the extraction stage ,the only parameter the extract or needs to know is the histogram shifting amplitude Δwhich parameterizes PHS as well as the classification processes Notice that in this scheme , the value of Δ is fixed by the user. Message extraction is conducted independently in each region and pass. For the PHS message, the extract or will retrieve by itself the values of T_{min} and T_{max}.

After Pixel Histogram Shifting Algorithm, Here is the Visual Cryptography Algorithm:

Step I: The source image is divided into n number of shares using k-n secret sharing visual cryptography scheme such that k number of shares is sufficient to reconstruct the encrypted image.

Step II: Each of the n shares generated in Step I is embedded into n number of different envelope images using LSB replacement.

Step III: k number of enveloped images generated in Step II are taken and LSB retrieving with OR operation, the original image is produced.

6.1 Data flow at Extraction level

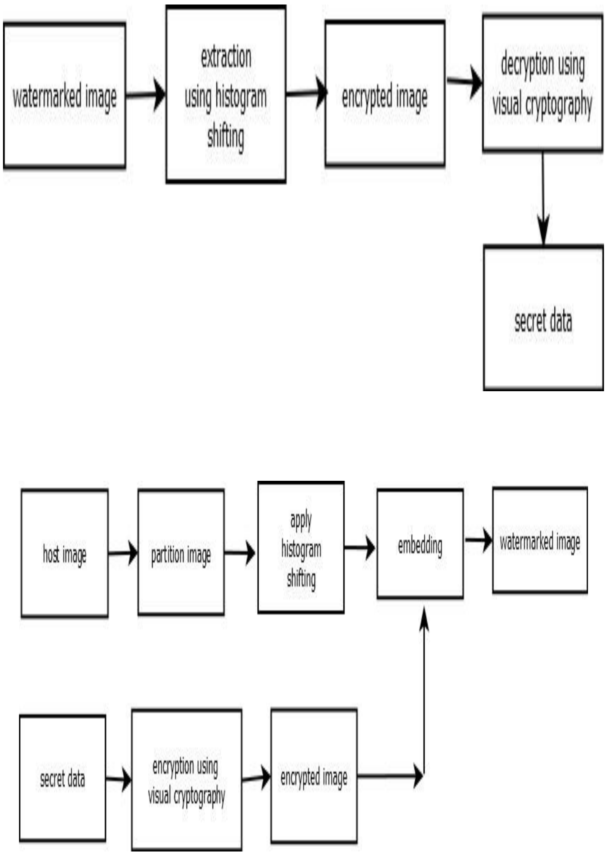


Fig 4. Data flow at eextraction level and embedding level

6. Experimental Result:

In this scheme to achieve performance, different criteria have to be considered:

--- Capacity rate C expressed in bpp(bit of message per pixels of image);

---Peak Signal to Noise Ratio (PSNR) so as to measure the distortion between an image I and its Watermarked version I_w

PSNR= 10log10

$$\left(\frac{NM\left(2^{d}-1\right)^{2}}{\sum_{i,j=1,1}^{N,M}\left(I\left(i,j\right)-I_{w}\left(i,j\right)\right)^{2}} \right)$$

Where d to the image depth and N and M to the image dimensions.

In this proposed work the experimental results will be given in terms of capacity and image distortion which depends on pixel shifting algorithm and no of times the image passes through algorithm. Result will be given in terms of capacity and distortion in the table format.

Let us take following images as example:

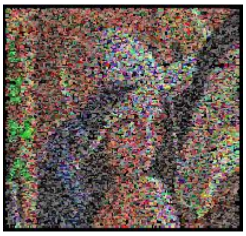
Fig 6. Natural Test Images: Lena

After applying Pixel Histogram Shifting Algorithm the Capacity and Distortion of the image will be compared with the other existing scheme, the result will look like this:After applying Pixel Histogram Shifting algorithm we have to apply Visual Cryptography, for this here we are applying digital enveloping techniques: k-n secret sharing visual cryptography scheme.

Original color Image:

Fig 7. Source Image

No. of shares will be 4but only 3 shares will be considered for experiment. Image shares produced will look like after applying visual cryptography:



7. Advantages And Limitations:

- It provides robustness due to Pixel Histogram Shifting algorithm as it provides good capacity and low distortion. Also it provides low peak signal to noise ratio.
- Image is well protected as we are using visual cryptography to secure the image from unauthorised users and protect the image from hackers. It is very useful in Military and medical area where security is prior issue.
- Better pixel prediction as both the algorithm provides high capacity and low distortion.

Limitations:

- Image is not protected in a correct way as if any share image is hacked we can not retrieved the original image
- Allows discontinuity in protection because of envelope as they have to encrypt and decrypt in similar sequence, if the sequence is changed at receiver level we can not get the original image as it is.

8. Conclusion

In this paper we will proposed a new reversible watermarking scheme which originality stands in identifying parts of the image that are watermarked using pixel histogram shifting and visual cryptography. As we are using here K-n shares visual cryptography technique, this will provide a protection against unauthorised attackers. This scheme offers a very good compromise in terms of capacity and image quality preservation for both medical and natural images. Pixel histogram shifting will provide the better way to identify the watermark and visual cryptography will help to encrypt the watermarked image and obtained original image.

Acknowledgment

I avail this opportunity to express my deep sense of gratitude and whole hearted thanks to my guide **Prof. S. A. Murab** of Jagadambha College of Engineering & Technology, Yavatmal for substantial guidance and cooperation in the seminar. He has provided all the facilities whenever I need and mostly for his gracious encouragement, advice and guidance. I also express my gratitude to **Prof. Dr. M. V. Sarode**

Head, Department of Computer Engg. And **Prof. Dr. S. K. Kalaspurkar** Principal, Jagadambha College of Engineering & Technology, Yavatmal for constant inspiration and valuable advice.

Reference

1. 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.
2. 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.
3. J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003
4. 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.
5. 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.
6. H. M.chao, C. M. Hsu, and S. G. Miaou, "A data hiding techniques with authentication, integration, and confide-ntiality for electronic patient records," IEEE Trans. Inf. Technol. Biomed.,Vol. 6, no. 1, pp. 46-53, Mar. 2002
7. V. Sachdev, H. J Kim, S. Suresh, and Y.-Q. Shi, " Reversible watermarking algorithm using sorting and prediction, " IEEE Trans. Circuit Syst. Video Technol., no 7., pp. 989-999, jul. 2009.
8. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognit, vol. 41,pp. 35823591, 2008.
9. C.H. Yang and M. H. Sai, "Improving histogram-based reversible data hiding by Interleaving predictions, "IET Image Process, v.4, n. 4, pp. 223-234, Aug. 2010.
10. Moni Noor and Adi Shamir,"Visual Cryptography", in preceding of advances in Cryptography EUROCRYPT 94, LNCS V 950 pages. Springer-verlag 1994
11. G.S.Raman, C.Surya, R.Balaji Ganesh." Reversible Watermarking Based on Predictio Error Expansion and Pixel Selection on Color Image", International journal of Engineering and Advanced Technology, vol 2, Issue 4, April 2014.
12. Yongjian Hu, Heung-Kyu Lee, and Jianwei Li,"DE-Based Reversible Data Hiding With Improved Overflow Location Map", IEEE Transactions On Circuits And Stsyem For Video Tech, Vol. 19, No. 2, February 2009.
13. Shyja.T.V , N.A.Vidya Mol2 ," Reversible Watermarking Based on Optimal Dynamic Histogram Shifting", *International Journal of Engineering Research and Applications International Conference on Humming Bird (01st March 2014).*
14. Dr.Rajendra D.Kanphade and Mr.Navnath S. Narawade ," Robust Reversible Water-Marking For Geometric Attack by Proposed Pixel Replacement Method", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* Volume 2, Issue 1, January – February 2013.
15. S. Yousefil, H. R. Rabiee, E. Yousefi, M. Ghanbari, "Reversible Date Hiding Using Histogram Sorting and Integer Wavelet Transform", 2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies.
16. Te-Cheng Hsu, Alan Dahgwo Yein,"Reversible Watermarking Algorithm Based on Embedding Pixel Dependence", Journal of Internet Technology Volume 13 (2012) No.4.

17. L. Kamstra and H. J. A. M. Heijmans, " Reversible Data Embedding Into Images Using Wavelet Techniques and Sorting", IEEE Transactions on Image Processing.Vol-14 December 2005.
18. H.J. Hwang, J. Kim, V. Sachnev and S.H. Joo, "Reversible Watermarking using optimal Histogram pair shifting based on prediction and sorting," KSII, Trans. Internet Inform. Vol. 4, no. 4, pp, 655-670, Aug, 2010.