Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-241-244
Available online at http://www.bioinfo.in/contents.php?id=55

REVERSIBLE WATERMARKING OF MEDICAL IMAGES: AUTHENTICATION AND RECOVERY-A SURVEY

MANDEEP KAUR[1] AND RUPINDER KAUR[2]

University Institute of Engineering and Technology, Panjab University, Chandigarh
*Corresponding Author: Email– [1]mandeep24@gmail.com, [2]rupinder.kaur040@gmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- The integrity of the medical images is crucial requirement for the diagnosis of patient's disease. Therefore, how to retain the validity between images and medical records is an important topic of research and real applications. The watermarking techniques can be used to maintain the integrity, authenticity and also drastically reduce the data storage requirement of medical records. Among different kinds of digital watermarking schemes, reversible watermarking has become a research hotspot. It is also called lossless data embedding as it embeds (hides) data (or payload) into a digital image in a reversible fashion [3]. Being reversible, the original digital content can be completely restored. It is a critical requirement for medical images, as its diagnostic value should not been compromised. Due to many research advances in the field of reversible watermarking, it has become very difficult to judge an appropriate algorithm for watermarking of different medical image modalities. In this paper, we present a comprehensive study of all basic reversible watermarking techniques applicable for medical images.

Keywords- authenticity, reversible watermarking, data embedding, medical records, payload.

Citation: Mandeep Kaur and Rupinder Kaur (2012) Reversible Watermarking of Medical Images: Authentication and Recovery-A Survey. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-241-244.

Introduction

Most hospitals and health care systems involve a large amount of data storage and transmission, such as administrative documents, patient information, medical images, and graphs. Among these data, the patient information and medical images need to be protected against any malicious attempts. To prevent patient's information from any attack, three things are required i.e. Integrity, Privacy and Authenticity of medical records. To maintain the privacy, patient data can be embedded into the medical images. After data embedding, the output image should be as similar as its original image so that doctors can perform proper treatment by using the images with hidden data when necessary. Thus, how to preserve the integrity of the medical image is another important issue. And thirdly, due to the vast amount of images, when the medical doctor needs to retrieve Patient #1's images along with his/her medical records, Patient #2's images may unexpectedly be obtained by the doctor even though this kind of probability is minute. And this means that the correlation between the medical images and medical records of the same patient should be authenticated, and then the doctor can proceed with the diagnosis procedures [4]. So there is a need to embed watermark in the medical images. Digital watermarking is a process of embedding valuable information into another digital media called host for the purpose such as copy control, authentication, copyright protection and distribution tracking.

To fulfill the need of privacy, integrity and authenticity we can use the data hiding scheme for receiving correct information and providing proper treatment to the patients .Reversible data hiding is a new branch in watermarking researches. In conventional watermarking techniques only the watermark needs to be extracted and examined at the receiver but reversible data hiding requires that both the hidden data and the original multimedia should be perfectly recovered. Data hiding or watermarking is a way to effectively embed the secret data into the cover media, including audio, video, and image. With the major purposes for copyright protection or data authentication, its process usually introduces irreversible degradation of the original multimedia. Reversible watermarking has found a huge surge of experimentation in its domain in past decade as the need of recovering the original work image after extracting the watermark arises in medical field. The reversible watermarking [2] not only provides authentication and tamper proofing [3] but also can recover the original image from the suspected image. With the term of "reversibility," it means that data, including patients' private information and the diagnosis data can be hidden into the medical image by some means. Later on, the medical image containing data might be retrieved by medical doctors while necessary, and both the original image and the hidden data can be perfectly recovered with the algorithm corresponding to the embedding scheme [5].

Reversible Watermarking Scheme

There are dozens of reversible watermarking techniques which have been reported in the literature and classified into different categories like reversible watermarking based on lossless compression, Difference Expansion scheme, Histogram shifting scheme and Interpolation Technique. Reversible watermarking schemes based on lossless data compression use the coding redundancy in images. They compress image data so that it takes less space and use the remaining space to embed watermark data. These schemes are generally computationally complex and their capacity is relatively small [2]. But other techniques are better in both of criteria.

Difference Expansion, is a kind of integer wavelet transform, was first proposed by Tian [3]. By expanding the difference between the two neighboring pixels of pixel pairs, Tian explored the redundancy in digital images to achieve a high-capacity and low-distortion reversible watermarking. The DE scheme modifies the relationships between two adjacent pixels. Under the predefined constraints that pixel values should lie between 0 and 255, by slightly adjusting the luminance value of adjacent pixels, data can be hidden into original image. A very large amount of data can be embedded, while a considerable amount of side information, indicating the locations suitable for hiding data, can be produced.

The histogram-based scheme takes the whole image into account for performing data hiding, and it modifies the distribution of histogram of image to hide data. Very few amount of overhead is generated [4].

This paper is organized as follows. In Section 2, we describe Difference Expansion Scheme. In Section 3, we propose Histogram Technique. In Section 4, we present Interpolation Technique. Finally in Section 5, we present our conclusion.

Difference Expansion

This scheme uses the inter-pixel redundancy that exists in natural images. In Difference Expansion Reversible data embedding scheme, we calculate inter-pixel difference and select some difference values for difference expansion (DE).Then the original content and payload (Patient’s data) will be embedded into the difference values. After that the watermarked image is reconstructed by using the modified values.

Calculation of Difference Expansion

Step1: Divide the original image into pairs of pixel values. Take two adjacent pixel values of x and y.

Step2: Calculate luminance difference and average values of pixels. Average value (l) denotes low frequency and difference value (h) denotes the high frequency. The difference value (h) is represented into its binary form.

Step3: Embed data bit b into the difference value after the least significant bit (LSB).This reversible data embedding operation h’=2 * h + b is called Difference Expansion

Data Embedding Phase

During data embedding all changeable difference values are modified by adding a new Least Significant Bit(LSB) through DE.

Data Embedding Algorithm consists of six steps:

Step1: Calculate the difference values by grouping the image into pairs of pixel values.

Step2: Divide these difference values into four disjoint sets: EZ (all expandable values of h), EN(all expandable h),CN(contains all changeable h), and NC(contains all non-changeable h):

Step3: Create a location map of selected expandable difference values. The location map gives the location information of all expanded difference values. Assign values to the location map. Value 1 denotes selected expandable difference value and 0 represents not selected expandable difference value.

Step4: Collect original LSBs of difference values.

Step5: Embed the location map, original LSBs and payload.

Step6: Apply the inverse integer transform to obtain the embedded image.

Data Extraction Phase

The extraction process consists of five steps:

Step1: Calculate the difference values. For an image, we do the pairing using the same pattern as in the embedding, and apply the integer transform to each pair.

Step2: Next we create two disjoint sets of difference values, CH, and NC:

- CH: contains all changeable h.
- NC: contains all non-changeable h.

Step3: Collect LSBs of all difference values.

Step4: Decode the location map by decoder.

Step5: The last step is content authentication and original content restoration. Apply the inverse integer transform to reconstruct a restored image. To authenticate the content, authentication hash is compared with the hash of the restored image. If they match exactly, then the image content is authentic, and the restored image will be exactly the same as the original image.

Advantage of Difference Expansion: Tian’s scheme [3] can achieve high capacity and also needs less computational power.

Disadvantage of Difference Expansion: The major drawback of Difference Expansion is the lack of capacity control , which results from having to embed the compressed location map along with the payload. The locations selected for expansion embedding determine the location map, so the compressibility of the location map depends on the set .Since it is impossible to predict the size of the compressed location map while selecting the locations to embed; it is difficult to determine the capacity before hand. Also, at low embedding rates (i.e., when only a few of the available expandable locations are selected), the compressibility of the resulting location map is low, resulting in a large fraction of the selected capacity to be allotted towards embedding the compressed map.

Histogram Reversible Data Embedding

The former technique of reversible watermarking is not robust under image processing and distortions. In order to enhance the robustness of the reversible watermarking, the embedding target is replaced by the histogram of a block. This scheme uses maximum and zero (or minimum if no zero points are available) points of histogram of image and shifts the values between these points. It considers the global characteristics of original image. Part of the histogram is intentionally altered to perform data hiding. It is described by the following steps.

Data Embedding Process

Step1. *Histogram Generation*: Produce histogram of original image. Luminance pixels with the maximal occurrences in histogram are labeled as max point and no occurrences in histogram are labeled as zero point.

Step2. *Range assignment*: Select the range between max and zero points.

Step3.*Modify Luminance values*: In the range between max and zero points, luminance values are modified accordingly.

- If the luminance value of the max point is smaller than that of the zero point, all the luminance values within this range would be increased by 1.
- If not, luminance values within the assigned range would be decreased by 1.

Step4.*Data embedding*: For the embedding of binary message, if the message bit is '1,' the luminance value is increased by 1; if the message bit is '0,' it is decreased by 1.

Data Extraction Process

Step1. *Histogram generation:* Receiver generates the histogram of image received from the sender side.

Step2. *Range assignment with side information:* Compare the luminance values between the max and zero points.

Step3. *Hidden data extraction:* Examine every pixel in the output image sequentially to extract the data bits with Step 4 of the embedding procedure.

Step4. *Original image recovery:* Original image is obtained by moving the histogram into its original form.

Although this scheme was an effective technique due to its ease of implementation and little side information produced but it required that some additional information be transmitted to receiver separately from watermarked image. Another drawback with histogram technique is that capacity is constrained by the occurrences of max point and how to get the increased capacity is another important issue for researches [4].

Advantages and drawbacks between histogram-based and DE methods

We summarize the advantages and drawbacks of both methods on the basis of amount of overhead and payload.

Amount of overhead: For the histogram-based method, the overheads are the luminance values of both the peak and zero points, meaning 2 bytes of side information [6] [7]. For the DE method and its variants, the location map plays an important role in extracting the hidden data and recovering the original, which depends on the characteristics of the cover medium. The location map serves as the side information, and its size is large, which is proportional to the data payload [5][8].

Data payload: For the histogram-based method, the data payload is constrained by the maximal number of occurrences in the histogram. For a pixel represented by 8-bit, with the luminance values ranging from 0 to 255, the maximal number of occurrences is generally below 10% of the total number of pixels, or 0.1 bit-per pixel (bpp) [7]. On the other hand, for the DE scheme, the data payload can be as high as 0.5 bpp, since every pair of consecutive pixels can carry 1 bit information [3].

Interpolation Technique

Interpolation technique is a method for guessing a pixel value from its surrounding. This technique provides low distortion and high embedding capacity than Difference Expansion and Histogram data embedding techniques. This technique can embed a large amount of covert data into images with imperceptible modification.

Interpolation-error expansion is a kind of DE. But it is different from most DE approaches in two important aspects[2]:

1) It uses interpolation-error (the difference between pixel value and its interpolation value) to embed data instead of inter-pixel difference used in Difference Expansion Scheme.

2) It expands difference, which is interpolation-error by addition instead of bit-shifting.

In this technique, two sets of pixels are used: sample pixels and non-sample pixels. A low resolution version of image is constructed using sample pixels and then non-sample pixels are interpolated. Finally the difference between this interpolated image and the original image is calculated—we call it "interpolation error". Because only non-sample pixels' values are interpolated and sample pixels retain their original values, if non-sample pixels are watermarked and sample pixels are kept unchanged during embedding, we will be able to get the exact same interpolated image from watermarked image.

Data Embedding Phase

Interpolation technique is mainly composed of two parts for the embedding the watermark: interpolation and embedding. In the interpolation process, we estimate the interpolated values and calculate the interpolation-errors in the raster scan. In the embedding process, we apply additive expansion to interpolation errors and embed the watermark information. The detailed description of the embedding process is given as follows.

1) Record some original LSB bits of the marginal area as overhead and add "0" to the beginning of boundary map as a label. Then, assemble overhead and watermark information to form payload.

2) Using (1), calculate interpolation-errors of the non-sample pixels.

3) Find the frequency of every interpolation-error and scan the cover-image from the beginning and start to undertake the embedding operation.

4) If x € {0,255}, put a "0" into the boundary map and move to the next one. Else, expand through additive expansion and work out the watermarked pixel x''. If x'' € {0,255}, put "1" into the boundary map.

5) For convenience, let C1 denote the condition when W is not completely embedded, and C2 denote the condition when the current pixel is not the end of non-sample pixels. If C1and C2are both satisfied, go to Step 4. If C1 is satisfied but C2 is not satisfied, record the length of the boundary map. Then, calculate the interpolation-errors of the sample pixels and go to Step 3.

6) Embed boundary map into marginal area of the cover-image using LSB replacement.

Data Extraction Phase

Data extraction process is described as follows:

1) Obtain boundary map from the LSB of marginal area of the watermarked image. Next, scan the watermarked image.

2) Extract the first bit of the boundary map, if it is equal to 0, go to Step 5.

3) Using (1), find the expanded interpolation-errors of the watermarked sample pixels. If x2 € {1,254}, recover the interpolation-error through inverse additive expansion. Else, x2 € {0,255}, remove the L th bit from boundary map. Do this step until the latter part of payload is extracted.

5) Using (1), calculate the expanded interpolation-errors of the watermarked non-sample pixels.

6) Decode overhead information and restore the pixels in marginal area once their LSBs are extracted.

7) Go to Step 6 if the former part of payload is not completely extracted.

8) Merge the bits in W1 and W2 to form the watermark information.

Advantages of Interpolation Technique

1. The distortion of image is smaller as since each pixel is altered at most by 1.

2. No location map is needed to tell between expanded interpolation-errors and non-expanded ones since they are

3. Interpolation-errors are more expandable than inter-pixel differences or prediction-errors because this scheme utilizes the full-enclosing pixels to interpolate the target pixel, so the interpolation-error tends to be smaller, which means that we can obtain a higher capacity.

4. Interpolation scheme provides a higher capacity and achieves better image quality for watermarked images.

5. The computational cost of the proposed scheme is small.

6. Due to the slight modification of pixels, high image quality is preserved.

Different from the latest schemes, the proposed scheme uses an interpolation technique to generate residual values names interpolation errors. By applying additive expansion to this interpolation-error, we achieve a highly efficient reversible watermarking scheme, which can guarantee high image quality without sacrificing embedding capacity. According to the experimental results, the proposed scheme provides a higher capacity and achieves better image quality for watermarked images.

Conclusion

Reversible watermarking is suitable for medical images, because this kind of media do not allow any losses. In this paper, we have given a detailed discussion on three reversible data hiding techniques. These are difference expansion-based reversible data hiding technique, histogram shifting-based reversible data hiding algorithm, interpolation error-based reversible data hiding scheme. The basic procedure, including the data embedding and the data extraction have been illustrated. The presented techniques not only provide authentication and tamper proofing but also can recover the original image from the suspected image. We have discussed all the above techniques based on PSNR and Embedding capacity and reach on a conclusion that interpolation technique has highest embedding capacity and it provides better image quality than that of Difference Expansion Scheme and Histogram Shifting scheme. So, we have to maintain an optimum balance between them to get a satisfactory result.

References

[1] Feng J.B., Lin I.C., Tsai C.S. and Chu Y.P. (2006) *International Journal of Network Security,* vol. 2, no. 3, pp. 161-171.

[2] Lain Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, Zhang Xiong (2010) *Information Forensics and Security, IEEE Transactions*, vol.5, no.1, pp.187-193.

[3] Tian J. (2003) *IEEE Trans.Circuits Syst.Video Technol*, vol 13,no.8,pp.890-896.

[4] Hsiang-Cheh Huang and Wai-Chi Fang (2011) *IEEE/NIH Life Science Systems and Applications Workshop*.

[5] Coltuc D. and Chassery J.M. (2007) *IEEE Signal Process. Lett.*, vol.14, no. 4, pp. 255–258.

[6] Kim H.J., Sachnev V., Shi Y.Q., Nam J. and Choo H.G. (2008) *IEEE Trans. Information Forensics and Security*, vol. 3, no. 3, pp. 456–465.

[7] Ni Z., Shi Y.Q., Ansari N. and Su W. (2006) *IEEE Trans. Circuits Syst, Video Technol.*, vol. 16, no. 3, pp. 354–362.

[8] Thodi D.M. and Rodriguez J.J. (2007) *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730.

[9] Alattar A.M. (2004) *IEEE Trans. Image Process.*, vol. 3, no.8, pp. 1147–1156.

[10] Hwang J., Kim J.W., and Choi J.U. (2006) *Int. Workshop on Digital Watermarking, LectureNotes in Computer Science*, *Jeju Island, Korea,* vol. 4283, pp. 348–361, Springer-Verlag.

[11] Tsai P., Hu Y.C. and Yeh H.L. (2009) *Signal Process.*, vol. 89, pp. 1129–1143.

[12] Fridrich J., Goljan M. and Du R. (2002) *EURASIP J. Appl. Signal Processing*, vol. 2002, no. 2, pp. 185–196.