



LOSSLESS IMAGE WATERMARKING METHOD BASED ON LOCAL PREDICTION

G.Ramachandran¹, PM Murali², S.Kannan³, T.Muthumanickam⁴, V.Maheswaramuniraj⁵

¹⁻³ Assistant Professor, Department of Electronics and Communication Engineering

⁴ Professor, Department of Electronics and Communication Engineering

¹⁻⁴ VMKV Engineering College, VMRF, Salem, Tamilnadu, India

⁵ Assistant Professor, Department of Electronics and Communication Engineering

⁵ Dr. Nallini Institute of Engineering & Technology, Palani road, Dharapuram. Tirupur, Tamil Nadu, India

Abstract: Lossless or Reversible watermarking is technique to hide the secret information in an image and to reconstruct the original image after the extraction of the watermark. The classical watermarking introduces permanent distortions; reversible watermarking not only extracts the embedded data, but also recovers the original host signal/image without any distortion. So far, three major approaches have already been developed for image reversible watermarking. They are reversible watermarking based on lossless compression, on histogram shifting and on difference expansion. The use of local prediction in difference expansion reversible watermarking improves the quality of reconstruction. For each pixel, a least square predictor is computed on a square block centred on the pixel and the corresponding prediction error is expanded. The same predictor is recovered at detection without any additional information. The proposed local prediction is general and it applies regardless of the predictor order or the prediction context. For the particular cases of least square predictors with the same context as the median edge detector, gradient-adjusted predictor or the simple rhombus neighbourhood, the local prediction-based reversible watermarking clearly outperforms the state-of-the-art schemes based on the classical counterparts.

Keywords: Embedded data, image. Watermark.

I. Introduction

The growth of the Internet along with the increasing availability of multimedia applications has spawned a number of copyright issues. One of the areas that this growth has fueled is that of digital watermarking. Digital watermarking is the general technique of embedding a blob of information in the original file, such that an altered file is obtained. The blob of information, thus included, serves one of different uses, such as, identifying piracy, sensing tampering, or reassuring integrity. The approaches to watermarking are diverse and can be broadly classified based on their visibility, robustness, or fragility. Their uses are also versatile, as they can be applied to text, images, audio, or video.

A) INTRODUCTION TO WATERMARKING

A digital watermark is defined as information embedded inside other chunks of information. The various types of watermarks can be better described by going through some of the most common purposes such as

Digital signatures – The watermarks holds information identifying the owner of the content.

Fingerprinting – The watermark hides information about the authorized user of the content.

Broadcast and publication monitoring – The watermark is used to monitor the use of broadcasted or published information, as in the Philips Research initiative of creating Visual Identity Verification Auditor (VIVA) “to investigate and demonstrate a professional broadcast surveillance system. Broadcast material will be pre-encoded with an invisible unique watermark identifier. Authentication – The watermark (or in this case also called a vapormark) is used to guarantee that the content showed is precisely the one created.

Copy control – This watermark records information regarding possibilities of reproduction of the data. It will store simple rules similar to “data cannot be copied” or “data can be copied once only, and never afterwards”.

Secret communication – If there is no suspicion, information could be hidden on a watermark and sent without detection. Rivest suggests that watermarking, as well as his proposed confidentiality method (chaffing) are completely different techniques from encryption and therefore such techniques effectively invalidate the strong efforts put on by the government to restrict encrypted communication as a national security issue. These methods can be as secure as encrypting information, if not more due to their unorthodox approach and unexpected character.

Captioning or visible logo – Watermarks can be used in video transmission as an extra channel of communication, transmitting information such as captions or a visible logo somewhere on the media. Watermark insertion and detection usually are symmetric. This means that whatever method used to insert the watermark

inside a file will be inversed to extract the watermark. This is illustrated in Figure 1.1. Any type of watermark insertion method, if probed long enough and with enough resources, will be broken. Therefore, if the information contained in the watermark is of absolute security, none of the available watermarking methods today could guarantee its embedding and detecting safely. The problem's core then becomes how secure should the watermark be. This degree of security will vary depending on the type of watermark used and the type of attack that is probable against it. Nowadays watermark design is tailored for the application and for probable attacks. The future works Biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been developed based on fingerprints, facial features, voice, hand geometry, handwriting, the retina, and the one presented in this thesis, the iris. Biometric systems work by first capturing a sample of the feature, such as recording a digital sound signal for voice recognition, or taking a digital colour image for face recognition and High Performance Iris Recognition Using Phase Based Image Matching [14] During the recognition phase the state history of length 20 image frames are determined for the moving object detected in the viewing range of the camera and Adaptive Edge Detection Algorithm For Flame And Fire Images [15]

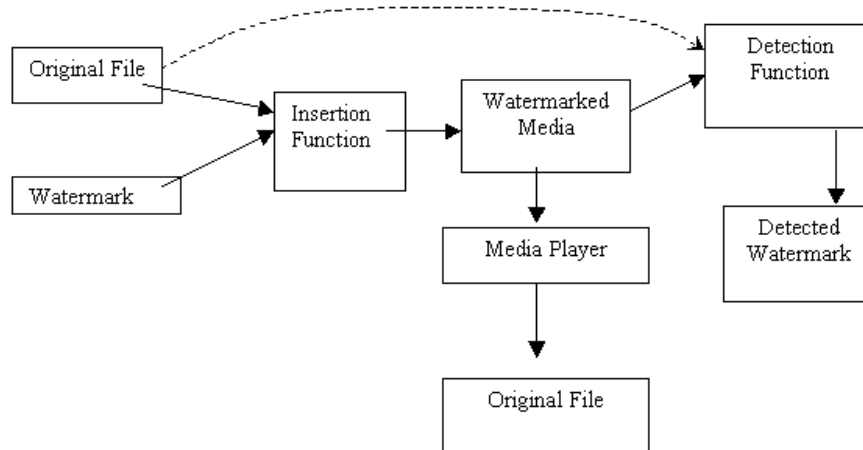


Figure 1.1 General watermark insertion/detection mechanism

II. Fonts Broad Classification of Watermarking

Watermarking techniques can broadly be classified based on their inherent characteristics: visible and invisible. Visible watermarks: A visible alteration of the digital image by appending a “stamp” on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity. Invisible watermarks: By contrast, an invisible watermark, as the name suggests that this is invisible for the most part and is used with a different motive. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and non-repudiation. Another way of classifying watermarking technique is a factor of its usage: robust, fragile, or semi-fragile, and spatial or spectral watermarks. Robust watermarks: Watermarks can be used to hold knowledge of ownership. Such watermarks need to remain steadfast to the original image to do what they advertise. The intactness of the watermark is a measure of its robustness. These watermarks must be able to withstand normal manipulations to the image such as reduction of image size, lossy compression of image, changing the contrast of the images, etc. Fragile watermarks: These are complementary to robust watermarks and are, as a rule, more change-sensitive than robust watermarks. They lose their mettle when they are subject even to the smallest changes. Their use lies in being able to pin-point the exact region that has been changed in the original watermarked image. The methods of fragile watermarking range from checksums and pseudo-random sequences in the LSB locale to hash functions to sniff any changes to the watermark.

Semi-fragile watermarks: These watermarks are a middle ground between fragile watermarks and fragile watermarks. They engulf the best of both worlds and are more resilient than fragile ones in terms of their robustness. They also are better than robust watermarks in terms of locating the regions that have been modified by an unintended recipient.

Spatial watermarks: Watermarks that are applied to the “spatial domain of the image” are said to be spatial watermarks.

Spectral watermarks: These are watermarks that are applied to the “transform coefficients of the image”.

III. Results and Discussions

The proposed watermarking algorithm is test on various gray scale images. The proposed method shows the improved embedding capacity of the images. The PSNR value of the images is also in the reasonable level which can be tolerated because of the increased embedding capacity. Table 5.1 shows the comparison of embedding capacity and PSNR of the proposed watermarking scheme.

Table 5.1 Parameter comparison of images

Input image	Barbara		Lena		Boat	
Embedding Capacity	75645(bits)		80231(bits)		78549(bits)	
Parameters	No of bits hidden	PSNR (dB)	No of bits hidden	PSNR (dB)	No of bits hidden	PSNR (dB)
Secret Sample 1	75000	27.1039	75000	29.1649	75000	28.1743
Secret Sample 2	55400	28.3782	55400	29.8965	55400	29.0435
Secret Sample 3	40800	28.9903	40800	30.6754	40800	29.8845
Secret Sample 4	25992	30.1515	25992	33.7012	25992	31.1417

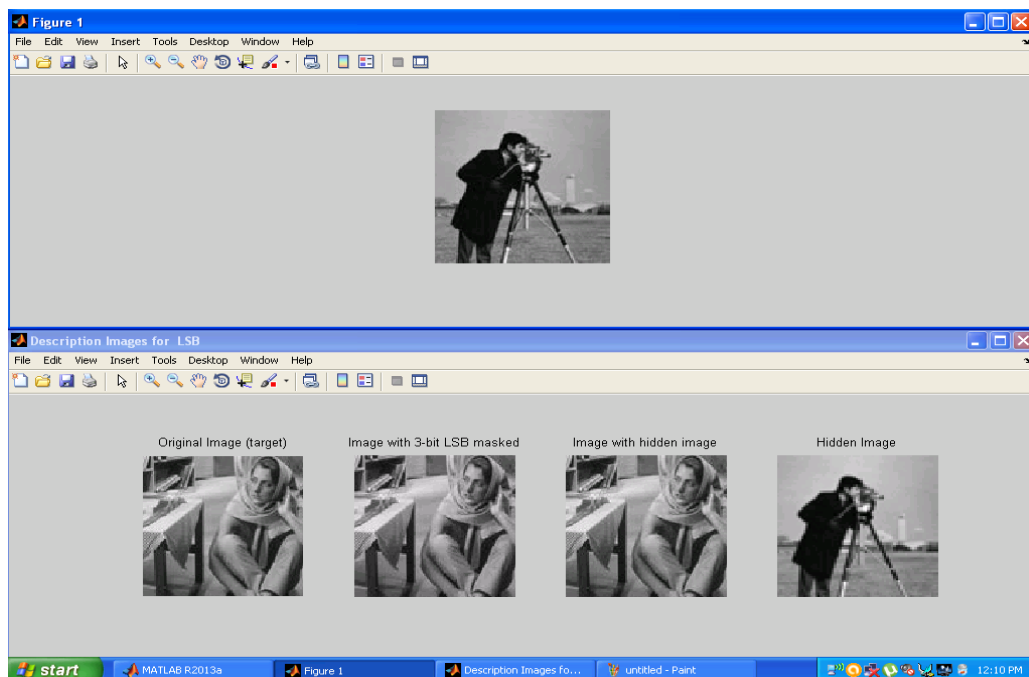


Figure 5.1

The Figure 5.1 shows the sample screen shot which uses a cameraman image as the secret information. This information is hidden in the Barbara image.

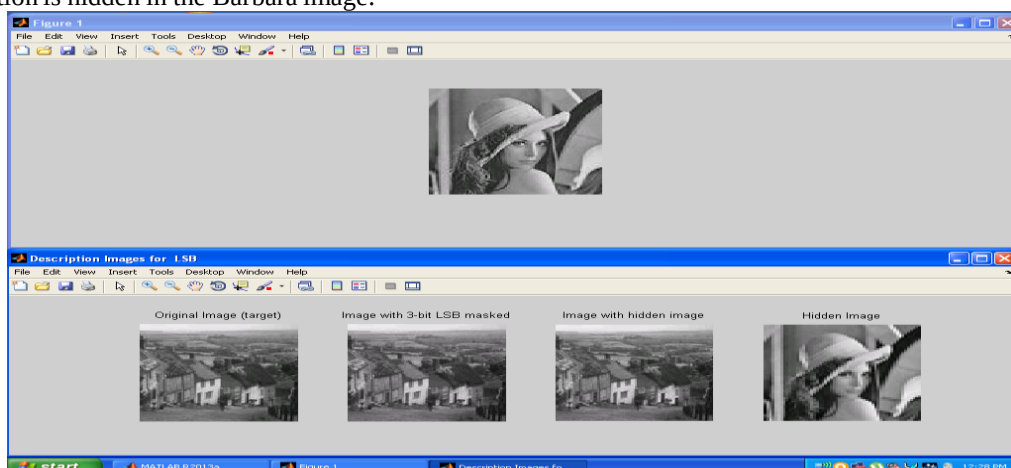


Figure 5.2 Sample screen shot2

The Figure 5.2 shows the sample screen shot which uses a Lena image as the secret information .this information is hidden in the boat image .From the comparison table it is clear that the original image which has higher mothness have the high PSNR value when compared with the other images.

IV. Conclusion

The use of local prediction based reversible watermarking has been proposed. For each pixel, the least square predictor in a square block centered on the pixel is computed. The scheme is designed to allow the recovery of the same predictor at detection, without any additional information. The local Prediction based reversible watermarking was analyzed for the case of four prediction contexts, namely the rhombus context and the ones of MED, GAP and SGAP predictors. The appropriate block sizes have been determined for each context. Among the four local prediction schemes analyzed, the one based on the rhombus context provides the best results. The results have been obtained by using the local prediction with a basic difference expansion scheme with simple threshold control, histogram shifting and flag bits.

References

- [1] Chang, C.-C., Fan, Y.-H., Tai, W.-L.: "Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery", IET Pattern Recognition, , vol 41, pp 654–661, August 2008, no. 6.
- [2] H.-J., Zhang, J.-S., Chen, F.: "Adjacent-block Based Statistical Detection Method for Self-Embedding Watermarking techniques", IEEE Conference on Signal Processing, pp 1557–1566, May 2009, no 8.
- [3] H., Chen, F., Tai, H.-M., Kalker, T., Zhang, J.: "Performance Analysis of a Block-Neighborhood-Based Self-recovery Fragile Watermarking Scheme", IEEE Signal Processing letters, vol 7, pp 185–196, September 2012, no 9.
- [4] Iwata, M., Hori, T., Shiozaki, A., Ogihara, A.: "Digital watermarking method for tamper detection and recovery of JPEG images". IET Signal Processing, vol 43, pp 309–314, march 2010, no 4.
- [5] Kundur, D., Hatzinakos, D.: "Digital watermarking for telltale tamper proofing and authentication", IEEE Image Processing, vol 87, pp 1167–1180, July 1999, no 9.
- [6] Kostopoulos, I., Gilani, S.A.M., Skodras, A.N.: "Colour image authentication based on a self-embedding technique". IEEE International Conference, Digital Signal Processing, vol 2, pp 733-736, may 2002, no 3.
- [7] Lu, H.-T., Shen, R.-M., Chung, F.-L.: "Fragile watermarking scheme for image authentication", IEEE Computer Graphics Image processing, vol 12, pp 898–900, October 2003, no 3.
- [8] Li, C.-T., Si, H.: "Wavelet-based fragile watermarking scheme for imageAuthentication", IEEE Computer Graphics Image Processing, vol 16, pp 130- 144, November 2007, no 4.
- [9] Lin, P.-L., Hsieh, C.-K., Huang, P.-W.: "A hierarchical digital watermarking method for image tamper detection and recovery", IEEE Image Processing, vol 38, pp 2519–2529, August 2005, no 3.
- [10] Lin, S.D., Kuo, Y.-C., Yao, M.-H.: "An image watermarking scheme with tamper detection and recovery", CVPR Image Segmentation, vol 3, pp 1379–1387, September 2007, no 4.
- [11] ILiu, K.C.: "Color image watermarking for tamper proofing and pattern-based recovery", IET Image Processing, vol 6, pp 445–454, April 2012, no 5.
- [12] Mirza, H., Thai, H., Nakao, Z.: "Color image watermarking and self-recovery based on independent component analysis", IEEE Watermarking Scheme, vol 67, pp 839–849, October 2008, no 3
- [13] S.Vaishnodevi, S.Kalaivani "High Performance Iris Recognition Using Phase Based Image Matching S.Vaishnodevi G.Sureshkumar,C. Arun kumar Madhuvappan, S.Mathankumar"Wireless Server For Total Healthcare System For Clients" International Journal of Applied Engineering Research" Volume 10 Issue Number 11 Pages9439-29444 Publisher Research India Publication
- [14] S.Vaishnodevi, S.Kalaivani" High Performance Iris Recognition Using Phase Based Image Matching" International Journal of Advance Research and Innovative Ideas in Education" Vol-1 Issue-1 2015 -ISSN(O)-2395-4396
- [15] K.Jayaram et al, "Adaptive Edge Detection Algorithm For Flame And Fire Images " International Journal Of Advance Research In Science And Engineering, Vol. No.3 , Issue No.01, January 2014 ISSN -2319-8354 ,page1-7
- [16] Ms T.Sheela etal,"RFID Based Automatic Ration Selling System"International Journal of Engineering, Business and Enterprises Applications (IJEBA), Issue 12, Volume 2, pp. 131-134, March-May, 2015 ,ISSN (Print): 2279-0020.