Vol. 3 No. 3 January 2016 ISSN: 2321 – 788X

DYNAMIC METHOD FOR IMPROVING THE RESISTANCE IN COMPRESSION BY USING WATERMARKING

J. Thasleen Fathima, MCA., M.Phil.,
Research Scholar and Assistant Professor, Dept of Information Technology,
HKRH College, Uthamapalayam, Theni – 625533

Abstract

Now-a-days watermarking plays a pivotal role in most of the industries for providing security to their own as well as hired or leased data. This paper its main aim is to study Spatial and Fractal watermarking algorithms and also choosing the effective and efficient one for improving the resistance in data compression. In the Spatial domain method, there is no costly transforms needed to be computed for watermark embedding. The luminance values will be manipulated directly. The fractal domain is to determine a set of contractive transformation to approximate each block of the image with a larger block. The composition of all these transformations has the image as its fixed point. Starting with any image hence to apply the composition of the transformations repeatedly and get an approximation of the original image.

For the implementation, we have used minimum nine coordinate positions. The watermarking algorithms to be taken for this study are Bruyn algorithm and Langelaar algorithm. In all graph, we have plotted X axis as peak signal to noise ratio (PSNR) and y axis as Correlation with original watermark. The threshold value á is set to 5. The result is smaller than the threshold value then it is feasible, otherwise it is not. From the results, we are trying to predict which technique is more suitable to which type of secret image.

Keywords*: PSNR, cover message, pixels, Manipulation, watermark*

Introduction

Digital watermarking is a method of embedding information in an image in such a manner that it cannot be removed. This watermark can be used for ownership protection, copy control and authentication. A digital watermark is a *secret message* that is embedded into a "cover message". Only the knowledge of a secret key allows us to extract the watermark from the cover message. A digital watermark can be visible or invisible. A digital watermarking is a method that uses a secret key to select the locations where a watermark is embedded.

Types of Watermarks

- **Visible watermarks** are designed to be easily perceived by the viewer, and clearly identify the owner; the watermark must not detract from the image content itself.
- **Fragile watermarks** are designed to be distorted or "broken" under the slightest changes to the image. *Semi-fragile watermarks* are designed to break under all changes that exceed a user-specified threshold. *Robust watermarks* withstand moderate to severe signal processing attacks on an image.

- **Spatial watermarks** are constructed in the image spatial domain, and embedded directly into an image's pixel data. *Spectral (or transform-based) watermarks* are incorporated into an image's transform coefficients. The spatial domain techniques directly modify the intensities or color values of some selected pixels.

Spatial Watermarkings

In the Spatial Domain algorithm, there is no costly transforms have to be computed for watermark embedding. There are three algorithms belongs to the category of spatial watermarking we have taken for our study. They are Kutter algorithm, Bruyndonckx Algorithm and Langelaar Algorithm. We have taken three algorithms in the category of fractal watermarking. They are bas algorithm, Puate Algorithm and Davern.

a. Kutter Algorithm

Here, the host image is not needed for extracting the watermark. The Watermark used here is a string of bits. Two leading bits are added to the mark: 0 and 1 bit. These two bits form a mini-template that will be used in the extraction process. It manipulates the values of the blue channel at single pixels. The pixels are visited in a zigzags path to get a sequence. Random site selection is used, but no qualitative site selection is done.

Figure 1: Watermark created by kutter

In the above figure, the strength of the watermark is dependent on the luminance of the host image.

b. Bruyndonckx Algorithm

The host image is not needed for extracting the watermark. It used a string of bits. It manipulates the luminance of zones of pixies in pixel blocks of size n x m.

To *embed* a bit into a certain block three steps are needed. They are

- **Classification**: The pixels in the block are to be divided into two zones of homogeneous luminance. The two blocks are a) blocks with hard or progressive contrast and b) blocks with noise contrast.
- **Subdivision**: Grids are applied to the block to divide the pixels into categories. A different grid is used for pixels in zone one and two. The grids have to remain secret, and are changed with every block.

- **Manipulation**: To divide the pixels in the block into 5 sets: some pixels have been discarded, the rest are either in zone one or two, and either in category A or B. The pixels in zone one are less luminous than those in zone two.

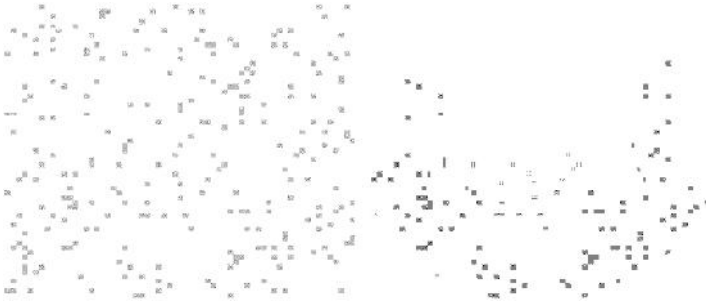


Figure 2: Watermark created by bruyndonckx

c. Langelaar Algorithm

In this algorithm, the host image is not needed for extracting the watermark. The Watermark used is a string of bits. This algorithm manipulates the luminance of pixels in 8 x 8 blocks. Random site selection is used, but no qualitative site selection is done.

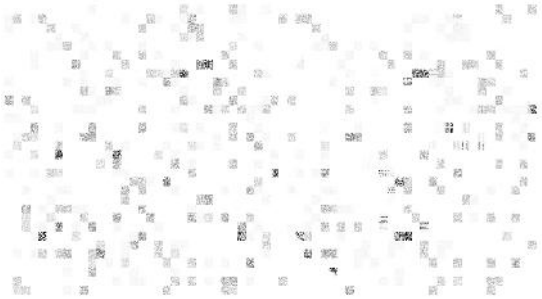


Figure 3: Watermark created by Langelaar

Fractal Domain Algorithms

This type of algorithm is to determine a set of contractive transformation to approximate each block of the image with a larger block. The composition of all the transformations has the image as its fixed point. Starting with any image hence to apply the composition of the transformations repeatedly and get an approximation of the original image.

a. Bas Algorithm

Ideas from fractal coding are used in this algorithm, but it also be classified as a spatial domain algorithm. It also mentions a wavelet domain method of embedding. To detect the host image is not needed to detect the watermark. The image is manipulated to contain certain self-similarities. Using this algorithm several *points-of-interest* are selected. Each points defines a 4 x 4 block centered around the point and 16 4 x 4 blocks, which form the domain pool.

To *embed* the watermark, for every point-of-interest the domain block with the same relative position to the point-of-interest is modified to be more similar to the range block than any other domain block.

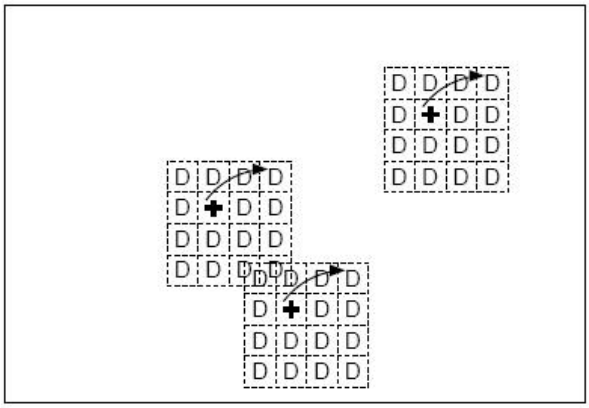


Figure 4: Blocks defined by the Points-of-Interest.

The number of matching blocks found is a measure of the probability that the watermark is in the image.

b. Puate Algorithm

It is described as a steganographical gorithm. Here the watermark is encoded in the image *format* rather than the image *data*. The host image is not needed to retrieve the watermark. If the image is converted to a different format (e.g. JPEG),the watermark cannot be retrieved. The watermark is a string of bits. A bit is embedded in the choice of transformation for a range block. The number of range blocks is an upper bound for the number of bits that can be embedded. The blocks are selected in pseudo random order, the knowledge about this sequence forms a secret key.

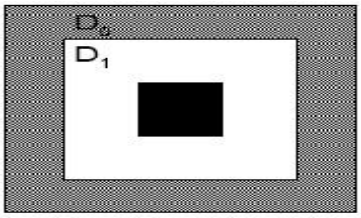


Figure 5: Dividing the domain pool

To *embed* the watermark, the domain pool *D* is divided into two sets $D_0$and D_1. To embed a bit into a selected range block r_i, a matching domain block is found in D_0 to embed a 0-bit, in D_1 to embed a 1-bit. By effectively shrinking the available domain pool to get less optimal matches, which results in a loss of image quality.

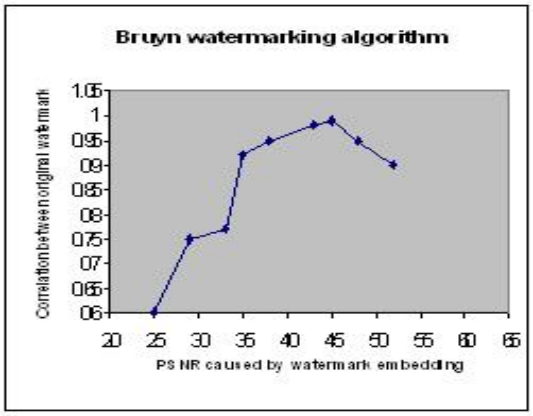
c. Davern Algorithm

Here, there is no data to show whether the algorithm is robust against attacks. The host image is not needed to retrieve the watermark. The watermark is a string of bits. The user manually selects two non-overlapping square regions of the image which will be called

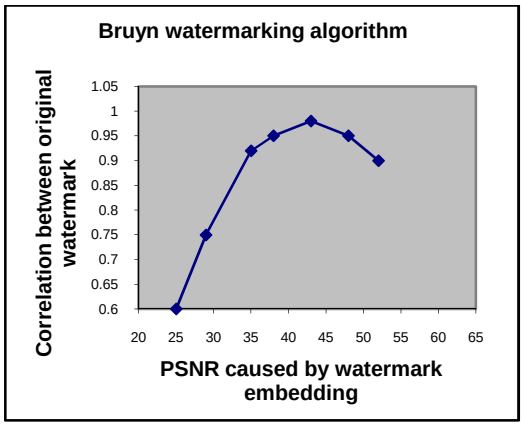
domain region and *range region*. The exact position of these regions will constitute part of the secret key needed to retrieve the watermark. Blocks in the range region are modified to embed a bit. These blocks may be of size 4 x 4, 8 x 8 or 16 x 16. The number of such blocks is an upper bound for the length of the watermark. The blocks are selected in pseudo random order, this forms the second part of the secret key.

Experimental Results

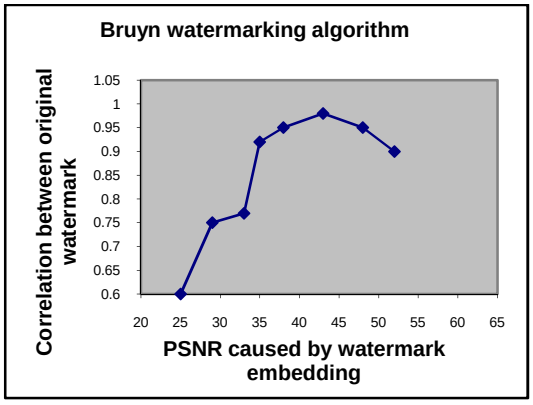
Bruyn Algorithm



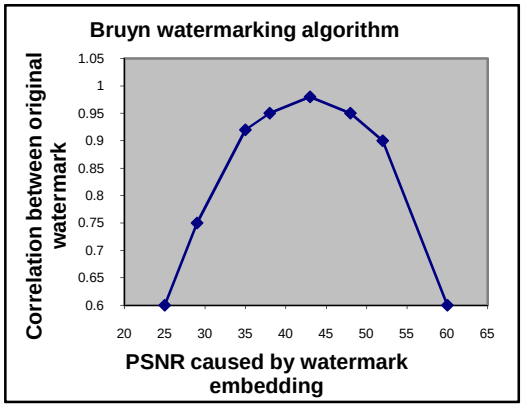
The original curve



After deleting the co-ordinate (33,0.77)



After deleting the co-ordinate (45,0.99)



After extending the co-ordinate (60,0.6)

Figure 6: Bruyn watermarking algorithm

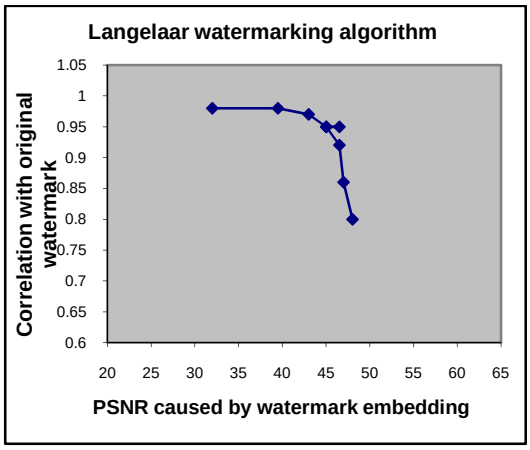
In this algorithm, the original curve started in the lower left corner of the graph. It is clearly understood that from the 6th co-ordinate position, the curve started its peak at right angled style i.e. 90^{o} position. The feature of the curve is slightly to a vertical curve because the edges drawn in the straight lines without any bends. Hence the curve view is not like a smooth normal distribution, because the tip portion is very sharp in the curve (45,0.99). To reduce the noise by making smoothening the curve, First to delete the 7th co-

ordinate position i.e. (45,0.99). Second to delete the 3rd Coordinate position i.e. (33,0.77).Then to extend the last coordinate to meet in the X axis. Now the Curve makes smoother and its resemblance looks like a parabolic curve. In this stage the number of coordinates are Eight. The number of process finished for transformation process is three. So it does not exceed the threshold value ά. It forms a smooth normal distribution curve within the boundaries and within the three steps.

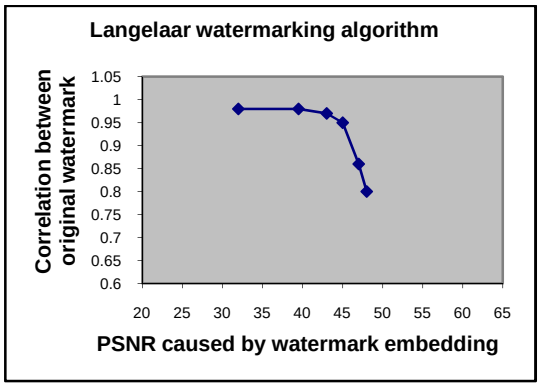
Langelaar Algorithm

In this algorithm, the original curve started from the upper left corner of the graph. It is clearly understood that the original curve looks like the ½ of the normal distribution curve. First to delete the 5th co-ordinate position i.e (46.5,0.95). Now the transformation process needs one Y-axis reflection i.e 180^0 rotation, and the change in position of an object that has been reflected about the line x = 0.

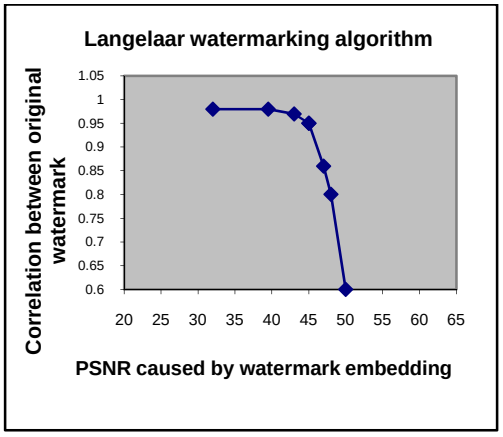
If needed we can extend the two edge coordinate positions for getting more smoother. Now the Curve makes smoother and its resemblance looks like a parabolic curve. In this stage the number of coordinates are Nine. The number of process finished for transformation process is four. So it does not exceed the threshold value ά. It forms a smooth normal distribution curve within the boundaries and within the three steps.



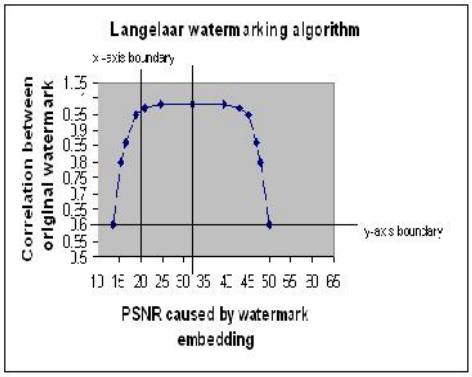
The original curve



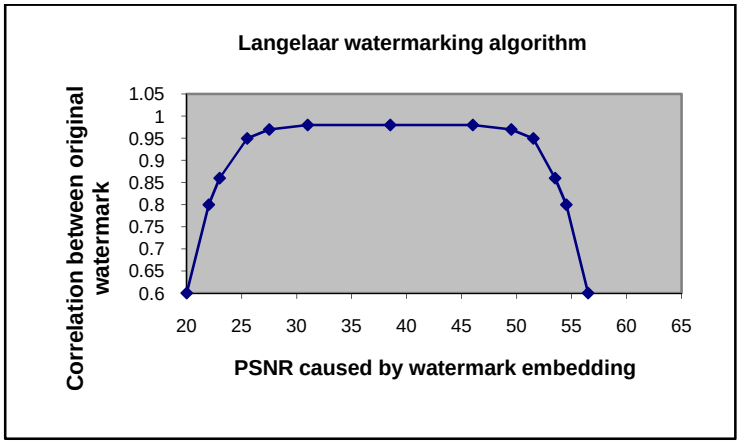
After deleting the co-ordinate (46.5,0.95)



After extending the co-ordinate (50,0.6)



After reflecting the curve from right side to left side using 180 degree rotation



After 6.5 value of the x-axis translation of the curve

Figure 7: Langelaar watermarking algorithm

Comparison between Bruyn and Langelaar

The Bruyn algorithm, the curves started from the lower left corner of the graph. But, in the Langelaar algorithm the curve starts from the upper left corner of the graph. Here all the three curves are with in the fixed threshold value (ά).

Using the Bruyn algorithm, it is formed a smooth normal distribution curve within the boundaries. Its reliability supportive ratio is 40%. So it is highly accepted. Next to Bruyn algorithm, the Langelaaralgorithm its performance is better.

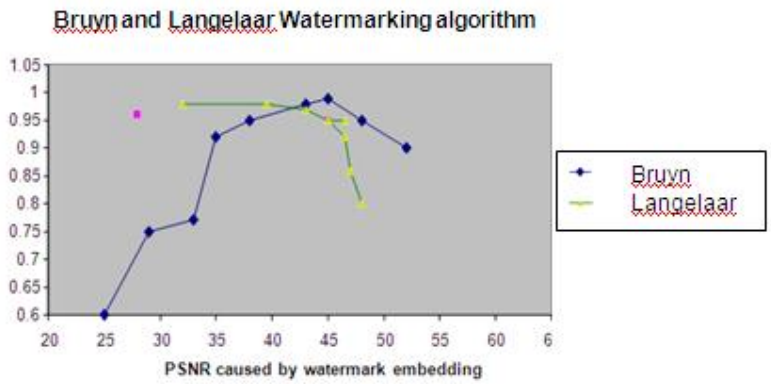


Figure 8: Before modification of Bruyn and Langelaar watermarking algorithm

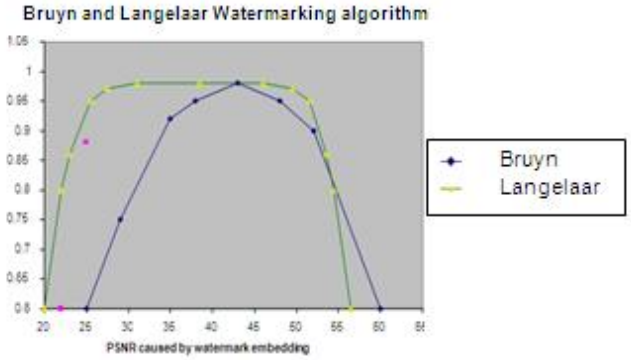


Figure 9: After modification of Bruyn&Langelaar watermarking algorithm

Conclusion

In this paper it is clearly understood that noise is unwanted thing for both text and images. This paper clearly identifies that comparatively the effective and efficient watermarking algorithm. The result displays that *Bruyn watermarking algorithm* is better than any other algorithm compared with Langelaar watermarking algorithm. As compared the Bruyn watermarking algorithm and Kutter watermarking algorithm, the former its efficiency is better for some cases and the latter its effectiveness is better for some cases. The main factor which influences to get the efficiency is “environment”.

References

1. R.C. Gonzalez and R.E. Woods, "Digital Image Processing", Addison-Wesley Publishing company, Inc., 2008.
2. B. Pfitzmann, "Information Hiding Terminology", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30 - June1, 2009, Lecture notes in Computer Science, Vol. 1174, Ross Anderson(Ed.), pp. 347-350.

3. F.A.P. Petitcolas, et al., "Information Hiding - A Survey", Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062-1078.
4. Hal Berghel, "Watermarking Cyberspace", Communications of the ACM, Nov. 2009, Vol. 40, No. 11, pp. 19-24.
5. F. Mintzer, et. al., "Effective and Ineffective Digital Watermarks", IEEE Intl. Conference on Image Processing, ICIP - 97, Vol. 3, pp. 9-12.
6. J. M. Acken, "How Watermarking Value to Digital Content?", Communications of the ACM, July 1998, Vol. 41, No. 7, pp. 75-77.
7. J. Cox and M. Miller, "A Review of Watermarking and Importance of perceptual Modelling", Proc. SPIE Human Vision and Imaging, SPIE-3016, Feb 2008.
8. R. Barnett, "Digital Watermarking: application, techniques, and challenges", IEE Electronics and Communication Engineering Journal, August 1999, pp. 173-183.
9. R.G. Van Schyndel, et. al., "A Digital Watermark", Proc. IEEE Intl. Conf. on Image Processing, ICIP-94, Vol. 2, pp. 86-90.
10. W. Bendor, et. al., "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996.
11. E. Franz, et. al., "Computer Based Steganography", Proc. First Intl. Workshop on Information Hiding, Cambridge, UK, May 30 - June 1, 1996, Lecture notes in Computer Science, Vol. 1174, Ross Anderson (Ed.).
12. F.A.P. Petitcolas, et al., "Information Hiding - A Survey", Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1062-1078.
13. J. Cox and M. Miller, "A Review of Watermarking and Importance of perceptual Modelling", Proc. SPIE Human Vision and Imaging, SPIE-3016, Feb 1997.
14. F. Mintzer, et. al., "Opportunities for Watermarking Standards", Communications of the ACM, July 1998, Vol. 41, No. 7, pp. 57-64.
15. G. Voyatzis and I. Pitas, "The Use of Watermarks in the Protection of Digital Multimedia Products", Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1197-1207.