Securing Images Using Watermarking Technique

Khalid Ahmed Ibrahim¹, G.K.Viju²

Abstract

Factors like Secrecy, Authentication, Non-repudiation and Integrity are considered in dealing with security. Watermarking is one such security measure. Watermarking technology generally permits authors to hide their names in the image behind their original work. In this proposed work, a segment based model is developed wherein the original image is partitioned into various segments and the information is made confidential. At the receiver's end the segments are combined to obtain the original image and the secret information. The model facilitates both watermark embedding and extraction. Besides copyright protection, authentication, security, digital watermarks can also serve as invisible labels and content links.

Keywords:- Authentication; Segmentation; Watermark embedding; Watermark detection.

مستخلص

يؤخذ في الاعتبار السرية والتوثيق وعدم الريبة والسلامة عن التعامل مع الامن والسرية. العلامة المائية هي احدي معايير الامن والسرية. تقنية العلامة المائية عموماً تسمح لمنشائنها من اخفاء اسمائهم في صورة خلف الاعمال الاصلية التي يقومون بها. في هذا البحث تم تطوير نموذج مبني علي تجزئة الصورة الاصلية الي قطاعات مختلفة تجعل المعلومات في غاية السرية عند الارسال. عند المستقبل يتم تجميع القطاعات المجزئة للحصول علي الصورة الاصلية حيث يقوم النموذج تضمين وفك العلامة المائية. بالاضافة الي حماية حقوق الطبع والنشر، التوثيق، الامن والسرية تعمل العلامة المائية كديباجات مخفية و رابط للمحتوي.

¹ Assistant Professor, Karary University, Sudan.

² Professor, Karary University, Sudan.

1. Introduction

Images of high resolution are generally composed of several homogeneous color regions, with color changes in adjacent pixels observed only at region boundaries. They may contain text or symbol content. Bit depth can vary, majority of such images use an 8 bit color map. The magnitude of the modifications made when embedding a watermark must be severely restricted. These watermarks have to be robust identifying synchronization errors and must have very high-resolution images. Embedding process includes several short, local noise signals to the boundaries between homogenous regions. Because signals are local, and their presence can be detected without reference to absolute position. Watermark detector is based on the correlation coefficient [1] and can efficiently search an image of several hundred million pixels for the presence of watermarks. Figure (1) and figure (2) show the flow of the watermark embedding and detection on the images.

Many of the watermarking techniques operate by modifying the coefficient produced by a transform of the image. They are difficult to apply images because the distortions induced by watermarking process introduce pixels that fall outside of the original image. Previously wavelet-based watermarking [3] technique is used so that the overall distortion did not exceed a fixed mean squared error threshold. But this does introduce colors outside the image's color map and is not robust to synchronization errors. Another technique, in which watermark given by a small binary image is embedded into a largest binary map image. Other schemes based on flipping selected bits [2] were used to detect tampering.

Figure (1): Flow Cart for Watermark Embedding

Figure (2): Flow Chart for Watermark Detection

2. Proposed Algorithm

In this work, the algorithm segments a color image to identify homogeneous regions of a specified color, and merges all pixel locations along the boundaries between segmented regions [8] into a list of candidate locations for watermark embedding. Watermark embedding algorithm adds multiple short, local watermark signals to the image by changing the color of pixels at locations selected randomly from among those locations along

region boundaries that meet a set of embedding criteria. Locality of the watermark signals allows them to be detected in the presence of errors such as shifting or cropping. The presence of watermark signals in an image is determined using a blind watermark detector that first segments the image, and then efficiently searches all region boundaries for the presence of watermark signals. Algorithm can efficiently process images of several hundred million pixels.

As given in the flowcharts the proposed algorithm takes in the watermark and the image and embeds the watermark into the image. While embedding it creates a boundary vector which will be used later while detecting the watermark. During the detection process, the watermark will be extracted from the watermarked image and a comparison is made with the boundary vector. The watermark seems to be correct; the algorithm outputs the watermark and the extracted image.

3. Image Segmentation

Watermark embedding and detection algorithms begin by identifying all contiguous, homogeneous regions of a specified color c , after which the region boundaries are extracted. Segmentation [9] produces a set of non-overlapping regions that are contiguous across rows. Algorithm processes rows from top to bottom while scanning within each row in a specified direction. Segmentation requires a set of regions S . The algorithm occupies less memory space where it has to store the current row, previous row and boundary information for all regions. First boundary of region S can be specified by location (X_s, Y_s) . Vector CS contains column locations of all

subsequent boundaries pixels in region S. Boundary can also be specified by a vector of differential values ds , whose elements are given by:

$$ds$$

$$n = cs$$

$$n - cs$$

$$n-1$$

Lds $\rightarrow$ length of the vector

3. Watermark Embedding

Length 'Lw' watermark vector 'w' is embedded into an image by first segmenting the image using a specified color and scan direction to extract the set of boundary vectors {CS} and the associated set of differential vectors {ds}. The watermark vector is then added to the vectors in the set {ds} at multiple locations to create a set of modified vectors {ds} which are used to construct a modified set of region boundaries.

5. Watermark Detection

Segmenting the candidate image performs detection and searching for locations with the watermark is highly correlated with the differential boundary vectors {ds}. All vectors in the set {ds} are concatenated into a single vector D. Here the detection threshold was determined prior to embedding the watermark by constructing the vector D from the segmentation of the original image and specifying detector threshold as $\hat{o} = \max n_{zcc}(\mathbf{w}, \mathbf{Dn})$.

5. Results

Watermarking algorithm was tested on a color image of resolution 10000x3000 taken from a database. Image had 21 distinct colors. The length $L_w = 75$ Watermark vector was constructed randomly concatenating vectors of length $l=3$. The detection threshold $\hat{\delta}$ was determined at the embedded and transmitted as side information. The watermark was embedded at 115 locations throughout the image into regions with color $c = 0$, which corresponded to black in the image's color map. The proposed algorithm embeds the watermark as given in figure (3).

Figure (3): Watermark Embedding

The figure shows the watermarked image and the watermark that is embedded into the image. And the watermark detection is given in the figure (4).

Figure (4): Watermark Detection

The figure shows the original image and the watermark detected from the image.

6. Conclusion

Using blind watermarking [4] a color-mapped maps a chart images. Algorithm embeds multiple short watermark signals into the boundaries between homogeneous regions. Watermarks are detectable when the images is shifted or cropped. Embedded watermarks [6] were shown to be robust to moderate levels of JPEG compression as well as to the addition of noise to the boundaries between regions. Algorithm efficiently process high-resolution map and chart images [7], which may have resolutions well in excess of 100 million pixels.

7. References

- [1] Lt.S.Santhoshbaboo,P.Subashini,K.S.Easwarakumar,B.SenthilKumar
“Digital watermarking for mobile and PDA devices based images”, GVIP
05 Conference, Egypt.2005.

- [2] I. Cox, J. Killian, F.T.Leighton, and T. Shamoon “Secure spread spectrum watermarking for multimedia”, IEEE Transactions on Image Processing **6**(12), pp. 1673–1687, 1997.
- [3] P. Vandergheynst, M. Kutter, and S. Winkler, “Wavelet-based contrast computation and application to digital image watermarking,” in Proc. SPIE Wavelet Applications in Signal and Image Processing Conference, pp. 82–92, (San Diego, CA), July 30–August 4, 2000. Invited paper.
- [4] P.-C. Su, C. Kuo, and H. M. Wang, “Blind digital watermarking for cartoon and map images,”in Security and Watermarking of Multimedia Contents, (San Jose, CA), January 1999.
- [5] M. P. Deseilligny and H. L. Men, “An algorithm for digital watermarking of binary images, application to map and text images,” in Proceedings of the International Workshop on Computer Vision, (Hong Kong), 1998.
- [6] M. Wu, E. Tang, and B. Liu, “Data hiding in digital binary image,” IEEE International Conf. On Multimedia and Expo (ICME), pp. 393–396, (New York, NY), 2000.
- [7] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, “A secure data hiding scheme for binary images,” IEEE Trans.Commun. 50, pp. 1227–31, August 2002.
- [8] A Watermarking Algorithm for Map and Chart Images Mark A. Masry Sibley School of Mechanical and Aerospace Engineering Cornell University, Ithaca, NY 14853
- [9] A.Said and W.A.Pearlman, “Anew, fast and efficient image Codec based on set partitioning in hierarchical trees”, IEEE Trans. On Circuits System, Video Technology Vol.6, pp.243-250, 1996.