Semantically Extended Digital Watermarking Model for Multimedia Content

Huajian Liu, Lucilla Croce Ferri, Martin Steinebach

Fraunhofer IPSI - Integrated Publication and Information Systems Institute,
Dolivostr. 15, 64293 Darmstadt, Germany
{liu, ferri, steinebach}@ipsi.fraunhofer.de
http://www.ipsi.fraunhofer.de/merit/

1 Semantically Extended Watermarking Model

Most current watermarking algorithms utilize syntactic features to achieve a good tradeoff between robustness and transparency by using perceptual models. They focus only on a detailed view of the contents, while little attention is paid to define and apply the semantic content features in the watermarking schemes.

However, in some specific watermarking applications, such current approaches show their limits. In order to satisfy different application goals, the semantic structure of the data, which gives an overall content understanding based on specific application goals, has to be taken into account as a fundamental part in the design of the watermark scheme. The concept of "region of interest" (ROI) has been integrated into specific watermarking algorithms, where the semantic meaning of a ROI depends strongly on the type and goals of the targeted application.

In this paper we propose an extended watermarking model based on semantic content understanding and illustrate its advantages. In the proposed model, the semantic and syntactic features in content understanding correspond respectively to different layers of the watermarking system, the application layer and the algorithm layer. On the first layer, the application decides the important levels of different regions of the content. Combined with content understanding, a content classification process is applied according to the retrieved underlying semantic features, in which the content is segmented into regions of more or less interest. Based on the importance levels, watermarks are embedded into different regions respectively, which are controlled by a visual model obtained from the syntactic features. The watermark messages could also be related to the different regions according to the specific application field. In the watermark detection process, the regions of various interests are obtained again by the content understanding and targeted application goals. The watermarks can then be retrieved from every watermarked region.

2 Advantages of the Semantically Extended Watermarking Model

First, the proposed semantically extended watermarking model can help in solving some open technical issues in the digital watermarking field. One of them is the resynchronization of watermark information during the detection process after geometric transformations. By applying a semantic content retrieval, the watermark detection algorithm can refer to the detected ROI positions, dramatically reducing the searching range and time and even directly finding the synchronization points. Another example can be an alternative solution to the problem of the permanent loss of data fidelity, caused by the most watermarking algorithms. For some special applications, extremely high fidelity requirements are specified. By applying image content understanding, different regions of an image can be identified with various importance levels, depending on the different application goals. The watermark can be embedded into the less important parts, avoiding affecting the fidelity of the most important parts, while the latter can still be protected by properly designing the watermarking scheme.

Furthermore, besides solving some technical issues, the “classical” functionality of digital watermarking can be extended by applying content understanding. For robust watermarking, such as copyright protection, the semantic watermarking model can enable the protection of specific objects with selective robustness to attacks, making object-based protection possible. For content integrity watermarking, semantic authentication can be achieved instead of only pixel-wise verification. Multiple security levels can be defined based on ROI specifications according to the different application goals.

As an application example, in our semantic watermarking scheme for human face images authentication [1], we consider human faces as objects of most interest and provide semantic protection with multiple levels of security in different regions. The application goal determines that the integrity of the face regions must be particularly ensured, including the position and quantity. A content understanding tool, the face detection algorithm [2], is applied to segment face regions from the background automatically. An authentication loop, embedded into the face regions, is defined to link all the faces together, while the background watermarks contain the total number of faces in the scene. In the watermark detection process, with the help of the located faces, the watermark synchronization can be achieved by an efficient local search even after slight background cropping. The highest security level is given to face regions and any adding, moving, changing and deleting faces are not allowed and will render the image unauthenticated. Background security level is lower compared to the face security. Content changing manipulations, caused by the common post processing, are allowed in the background, such as visual annotation and slight background cropping. Such semantic watermarking and multiple security levels partially enable to trace manipulations and to identify some kinds of attacks, which can help to infer the attacker’s motives.

References

1. H. Liu, H. Sahbi, L. C. Ferri, M. Steinebach: Advanced Authentication of Face Images. In Proceeding of WIAMIS 2005, Montreux, Switzerland, April, 2005
2. H. Sahbi, D. Geman, N. Boujemaa: Face Detection Using Coarse-to-fine Support Vector Classifiers. In Proc. of the IEEE Inter. Conf. on Image Processing, 2002, pp. 925–928