Blind Image Watermarking Using a Sample Projection Approach

ABSTRACT:

This paper presents a robust image watermarking scheme based on a sample projection approach. While we consider the human visual system in our watermarking algorithm, we use the low frequency components of image blocks for data hiding to obtain high robustness against attacks. We use four samples of the approximation coefficients of the image blocks to construct a line segment in the 2-D space. The slope of this line segment, which is invariant to the gain factor, is employed for watermarking purpose. We embed the watermarking code by projecting the line segment on some specific lines according to message bits. To design a maximum likelihood decoder, we compute the distribution of the slope of the embedding line segment for Gaussian samples. The performance of the proposed technique is analytically investigated and verified via several simulations. Experimental results confirm the validity of our model and its high robustness against common attacks in comparison with similar watermarking techniques that are invariant to the gain attack.

EXISTING SYSTEM:

In Existing block-based approach, in which the block size is constrained by 3* 3 pixels or larger, we process an image in 2* 2 pixel blocks. This allows flexibility in tracking the edges and also achieves low computational complexity. The two processing cases that flipping the candidates of one does not affect the flippability conditions of another are employed for orthogonal embedding, which renders more suitable candidates can be identified such that a larger capacity can be achieved.

PROPOSED SYSTEM:

We Proposed present a high-capacity data-hiding scheme for binary images authentication based on the interlaced morphological binary wavelet transforms. The relationship between the coefficients obtained from different transforms is utilized to identify the suitable locations for watermark embedding such that blind watermark extraction can be achieved. Two processing cases that are not intersected with each other are employed for orthogonal embedding in such a way that not only can the capacity be significantly increased, but the visual distortion can also be minimized. Results of comparative experiments with other methods reinforce the present scheme's superiority in being able to attain larger capacity while maintaining acceptable visual distortion and low computational cost.

The goal of authentication is to ensure that a given set of data comes from a legitimate sender and the content integrity is preserved .Hard authentication rejects any modification made to a multimedia signal ,whereas soft authentication differentiates legitimate processing from malicious tampering This paper focuses on hard authenticator watermark-based authentication.

Specifically, we investigate the problem of data hiding for binary images in morphological transform domain. Generally speaking, data hiding in real-valued transform domain does not work well for binary images due to the quantization errors introduced in the pre/post-processing In addition; embedding data using real-valued coefficients requires more memory space. The idea of designing an interlaced transform to identify the embeddable locations is motivated by the fact that some transition information is lost during the computation of a single transform and there is a need to keep track of transitions between two and three pixels for binary images data hiding. Specifically, we process the images based on 2 2 pixel blocks and combine two different processing cases that the flippability conditions of one are not affected by flipping the candidates of another for data embedding, namely "orthogonal embedding"

HARDWARE REQUIREMENTS

Hard disk	:	**40 GB**
RAM	:	**512mb**
Processor	:	**Pentium IV**
Monitor	:	**17''Color Monitor**

SOFTWARE REQUIREMENTS

Front-End	:	**VS .NET 2005**
Coding Language	:	**C#**
Operating System	:	**Windows XP.**

Modules :

1) Image as input
2) Watermark embedding
3) Authenticator Watermark
4) Swap Embedding
5) Watermarked Image

Modules Description :

1) Image as input :

We give image as input ,process an image in 2x2 pixel blocks. This allows flexibility in tracking the edges and also achieves high computational complexity. The two processing cases that flipping the candidates of one does not affect the *flippability* conditions of another are employed for *orthogonal embedding* .

2) Watermark embedding :

Watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark. Watermarked content can prove its origin, thereby protecting the data.

3) Authenticator Watermark :

In this module we encrypt the data embedded image.The purpose of authenticator watermark of a block is invariant in the watermark embedding process, hence the watermark can be extracted without referring to the original image .The encryption and decryption technices used in this module.

4) Swap Embedding :

We flipp an edge pixel in binary images is equivalent to shifting the edge location horizontally one pixel and vertically one pixel. A horizontal edge exists if there is a transition between two neighboring pixels vertically and a vertical edge exists if there is a transition between two neighboring pixels horizontally. We swap an morphological images.

5) Watermarked image

The watermarked image is obtained by computing the inverse for the main processing block to reconstruct its candidate pixels.use this module we going to see the original watermarked image.

REFERENCE:

Mohammad Ali, Sayed Mohammad Ebrahim Sahraeian and Craig Jin, "Blind Image Watermarking Using a Sample Projection Approach", **IEEE Transactions on Information forensics and security, April 2011.**