digital water mark

Overview

Digital watermarking refers to the embedding of specific information into a digital signal, which may be audio, picture or video. If a digitally watermarked signal is copied, the embedded information is also copied. Digital watermarks can be divided into two types: emergent and hidden. The former is visible watermarking, and the information contained in it can be seen at the same time when viewing pictures or videos. In general, floating watermarks usually contain the name or logo of the copyright owner. The example image on the right contains a floating watermark. The logo placed by the TV station in the corner of the screen is also a kind of floating watermark. Hidden watermarks are digital data added to audio, pictures or videos, but cannot be seen under normal circumstances. One of the important applications of hidden watermarking is to protect copyright, which is expected to prevent or prevent unauthorized copying and copying of digital media. Steganography is also an application of digital watermarking, and both parties can communicate using information hidden in digital signals. The annotation data in digital photos can record the time when the photo was taken, the aperture and shutter used, and even the brand of the camera, which is also one of the applications of digital watermarking. Some file formats can contain this extra information called "metadata".

nature

Security: Watermark information should be difficult to tamper with and forge. Concealment: The watermark is invisible to the senses, and the embedding of the watermark cannot affect the usability of the protected data, which is greatly reduced. Watermarks that do not have this feature are called Visible Watermarking. For example, when a TV station broadcasts a signal, its logo is often embedded in a corner. Robustness: The watermark can resist certain operations on the embedded data, and will not be wiped out by some subtle operations. Including individual bit errors generated in the transmission of data, image or video, audio compression. Watermarks that do not have this feature are called Fragile Watermarking. Watermark capacity: refers to the amount of information that a carrier can embed a watermark on.

Related technologies/tools

Mature watermark encryption tool

http://steghide.sourceforge.net/index.php Install: http://www.webm.in/2015/10/install-steghide-centos-6/ yum problem handling: http://wolfword.blog.51cto .com/4892126/1306203

Implementation of digital watermarking based on wavelet transform (Facebook)

Principle:
https://www.researchgate.net/publication/267988699_Image_Watermarking_Using_3-Level_Discrete_Wavelet_Transform_DWT slide:
https://www.slideshare.net/suritd/ppt1-48438386 Python Script: Features:

Use 2 wavelet transform;

Support watermark formats: image, text;

Support adding watermarks and dewatering watermarks;

Supports adding multiple watermarks to one image (to deal with screenshot/cut attacks).

Result：

origin_img

Scenarios where the watermark is an image:

Watermark:

python watermark.py --opt embedding --origin origin.png --watermark watermark.png --embedding embedding.jpg

Unpack the watermark:

python watermark.py --opt extracting --origin origin.png --embedding embedding.jpg --extracting extracting.jpg

watermark_img

embedding_img

extracting_img

Scenarios where the watermark is text:

Add multiple watermarks (against screenshot/cut attacks):

python watermark.py --opt embedding_word --origin origin.png --watermark_word 'lzh3lzh3' --embedding embedding_word.jpg --image_segments_num 2

Unpack the watermark:

python watermark.py --opt extracting --origin origin.png --embedding embedding_word.jpg --extracting extracting.jpg --image_segments_num 2

watermark_word: lzh3lzh3 (plus 2x2 watermarks)

embedding_img

extracting_img