Digital image watermarking resistant to geometric and removal attacks in the wavelet transform domain

Raymond Naegle and Xiaoxung Qi
Department of Computer Science, Mathematics, and Engineering, Shepherd University, Shepherdstown, West Virginia 25443
Computer Science Department, Utah State University, Logan, UT 84332

Introduction

In recent years, the Internet has become a staple of modern life. The increased penetration of broadband network access has made it easier for individuals to share information and communicate with one another. This increased ability to share data poses a threat to some copyright holders, whose intellectual property can be shared illegally. We present a blind watermarking scheme resistant to various commonly used removal attacks.

Methods

This work is based largely upon the work of Lee et al. [1,2]. The watermark is embedded in the image additively, in the Discrete Wavelet Transform (DWT) sub-bands. By exploiting the human vision system, as well as properties of the DWT, we are able to embed the watermark with varying weight to maximize signal strength, and minimize visibility. Since modern compression algorithms such as JPEG2000 use the DWT for compression, the watermark should be well preserved on a compressed image, and against removal attacks such as mean filtering.

To achieve invariance to various geometric attacks, the watermark signal is small and repeated periodically throughout the image — this allows any geometric attacks to be estimated and reversed by using a FFT-based auto-correlation function. The image is then checked for the presence of a watermark.

Results

Using the work of Lee and Lee [2] as a reference, we compare the strength of the watermarked image's raw autocorrelation peaks. These peaks are the single single most important element of the watermarking scheme, because of their importance in reversing geometric attacks.

On average, the strength of the raw ACF peaks is 11% stronger with our method.

Future Work

Intuitively, the added strength with which the watermark signal is embedded into the image should result in a higher percentage of positive watermark detections. Since this is ongoing research, we can not yet produce any data to substantiate to what degree this added embedding strength improves the probability of an accurate watermark detection.

Conclusions

Though somewhat computationally intensive today, image watermarking may become a feasible means for copyright holders to protect their assets in the future. We may also see a standardized watermarking scheme used in the future to protect content providers, such as YouTube, from litigation for unknowingly hosting copyrighted content by automatically screening marked content.

Other uses for this technology might include imaging software that embeds metadata into the pixel information of images, so that even when a document is printed and resanned, it retains additional information, without affecting image quality. Some examples of this metadata could include the date and time the photo was taken, by whom it was taken, and what kind of camera was used.

Methods (cont.)

By modifying a cover image's high-frequency noise, the image can be made to have the same periodic autocorrelation as our watermark pattern (1). This increases the resulting peak strength, which increases the probability that an attacked watermark image will still be correctly identified.

Any geometric attacks are reversed by constructing a triangle from the middle peak and it's two closest peaks on X and Y. An affine transformation is found that converts the modified triangle into it's original shape.

Geometric attacks that can be estimated and reversed include:
- Rotation
- Aspect ratio change
- Scaling
- Cropping
- Flipping
- Translation
- Row and column removal
- Combined rotation & scale

Methods

This work is based largely upon the work of Lee et al. [1,2]. The watermark is embedded in the image additively, in the Discrete Wavelet Transform (DWT) sub-bands. By exploiting the human vision system, as well as properties of the DWT, we are able to embed the watermark with varying weight to maximize signal strength, and minimize visibility. Since modern compression algorithms such as JPEG2000 use the DWT for compression, the watermark should be well preserved on a compressed image, and against removal attacks such as mean filtering.

To achieve invariance to various geometric attacks, the watermark signal is small and repeated periodically throughout the image — this allows any geometric attacks to be estimated and reversed by using a FFT-based auto-correlation function. The image is then checked for the presence of a watermark.

Results

Using the work of Lee and Lee [2] as a reference, we compare the strength of the watermarked image's raw autocorrelation peaks. These peaks are the single single most important element of the watermarking scheme, because of their importance in reversing geometric attacks.

On average, the strength of the raw ACF peaks is 11% stronger with our method.

Future Work

Intuitively, the added strength with which the watermark signal is embedded into the image should result in a higher percentage of positive watermark detections. Since this is ongoing research, we can not yet produce any data to substantiate to what degree this added embedding strength improves the probability of an accurate watermark detection.

Conclusions

Though somewhat computationally intensive today, image watermarking may become a feasible means for copyright holders to protect their assets in the future. We may also see a standardized watermarking scheme used in the future to protect content providers, such as YouTube, from litigation for unknowingly hosting copyrighted content by automatically screening marked content.

Other uses for this technology might include imaging software that embeds metadata into the pixel information of images, so that even when a document is printed and resanned, it retains additional information, without affecting image quality. Some examples of this metadata could include the date and time the photo was taken, by whom it was taken, and what kind of camera was used.

Methods

This work is based largely upon the work of Lee et al. [1,2]. The watermark is embedded in the image additively, in the Discrete Wavelet Transform (DWT) sub-bands. By exploiting the human vision system, as well as properties of the DWT, we are able to embed the watermark with varying weight to maximize signal strength, and minimize visibility. Since modern compression algorithms such as JPEG2000 use the DWT for compression, the watermark should be well preserved on a compressed image, and against removal attacks such as mean filtering.

To achieve invariance to various geometric attacks, the watermark signal is small and repeated periodically throughout the image — this allows any geometric attacks to be estimated and reversed by using a FFT-based auto-correlation function. The image is then checked for the presence of a watermark.

Results

Using the work of Lee and Lee [2] as a reference, we compare the strength of the watermarked image's raw autocorrelation peaks. These peaks are the single single most important element of the watermarking scheme, because of their importance in reversing geometric attacks.

On average, the strength of the raw ACF peaks is 11% stronger with our method.

Future Work

Intuitively, the added strength with which the watermark signal is embedded into the image should result in a higher percentage of positive watermark detections. Since this is ongoing research, we can not yet produce any data to substantiate to what degree this added embedding strength improves the probability of an accurate watermark detection.

Conclusions

Though somewhat computationally intensive today, image watermarking may become a feasible means for copyright holders to protect their assets in the future. We may also see a standardized watermarking scheme used in the future to protect content providers, such as YouTube, from litigation for unknowingly hosting copyrighted content by automatically screening marked content.

Other uses for this technology might include imaging software that embeds metadata into the pixel information of images, so that even when a document is printed and resanned, it retains additional information, without affecting image quality. Some examples of this metadata could include the date and time the photo was taken, by whom it was taken, and what kind of camera was used.

Methods

This work is based largely upon the work of Lee et al. [1,2]. The watermark is embedded in the image additively, in the Discrete Wavelet Transform (DWT) sub-bands. By exploiting the human vision system, as well as properties of the DWT, we are able to embed the watermark with varying weight to maximize signal strength, and minimize visibility. Since modern compression algorithms such as JPEG2000 use the DWT for compression, the watermark should be well preserved on a compressed image, and against removal attacks such as mean filtering.

To achieve invariance to various geometric attacks, the watermark signal is small and repeated periodically throughout the image — this allows any geometric attacks to be estimated and reversed by using a FFT-based auto-correlation function. The image is then checked for the presence of a watermark.

Results

Using the work of Lee and Lee [2] as a reference, we compare the strength of the watermarked image's raw autocorrelation peaks. These peaks are the single single most important element of the watermarking scheme, because of their importance in reversing geometric attacks.

On average, the strength of the raw ACF peaks is 11% stronger with our method.

Future Work

Intuitively, the added strength with which the watermark signal is embedded into the image should result in a higher percentage of positive watermark detections. Since this is ongoing research, we can not yet produce any data to substantiate to what degree this added embedding strength improves the probability of an accurate watermark detection.

Conclusions

Though somewhat computationally intensive today, image watermarking may become a feasible means for copyright holders to protect their assets in the future. We may also see a standardized watermarking scheme used in the future to protect content providers, such as YouTube, from litigation for unknowingly hosting copyrighted content by automatically screening marked content.

Other uses for this technology might include imaging software that embeds metadata into the pixel information of images, so that even when a document is printed and resanned, it retains additional information, without affecting image quality. Some examples of this metadata could include the date and time the photo was taken, by whom it was taken, and what kind of camera was used.