Novel Quality Metric for Improving Image Watermarking Techniques

S.Dhanalakshmi[1], T.Ravichandran[2]

[1]*Department of Computer Science & Engineering, SNS College of Technology, Coimbatore - 641 035, India*
dhana261978@yahoo.com

[2]*Department of Computer Science & Engineering, Hindusthan Institute of Technology, Coimbatore - 641 042, India*
t-ravichandran@gmail.com

Abstract— Image watermarking is applied in copyright management (copyright authentication, traitor tracing, and access control) as well as channel error resilience. Watermark are visible or not with a given watermark strength. However, the critical question is whether the watermark takes full advantage of the perceptual distortion constraint and achieves the robustness as high as possible.It proposes a second-order statistics (SOS)-based image quality metric, which considers the texture masking effect and the contrast sensitivity in Karhunen–Loève transform domain. Apply this metric for spread spectrum watermarking and quantization index modulation based watermarking techniques to minimize the distortion of the watermarked image and to maximize the correlation between the watermark pattern and the spread spectrum carrier as well as Quantization index modulation (QIM) carrier.

Keywords— Attacks, second-order statics , quantization index modulation.

I. INTRODUCTION

Image processing is any form of signal processing for which the input is an image such as a photograph or video frame, the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging.

Image watermarking is applied in copyright management as well as channel error resilience. Perceptual watermarking (except fragile watermarking) exploits aspects of the human visual system and seeks an invisible and robust watermark. Some work of perceptual watermarking does not rely on an explicit image quality metric. The upper bounds of watermark strength are set by the Just Noticeable Difference , which indicates the extent of a signal difference pattern being just perceived. These methods were usually testified by the subjective test on whether the watermark was visible or not with a given watermark strength.

Image quality assessment is a common problem for many applications including image restoration, coding, as well as watermarking. Image quality metric can be classified into full reference (FR), reduced reference, and no reference, according to the availability of the distortion free image (i.e., the cover image in watermarking), which may be used as the reference to evaluate the distorted counterpart. To minimize the distortion of the watermarked image and to maximize the correlation between the watermark pattern and the spread spectrum carrier.

II.RELATED WORKS

Steganography applications conceal information in other, seemingly innocent media. Steganographic results may masquerade as other file for data types, be concealed within various media, or even hidden in network traffic or disk space. This is only limited by our imagination in the many ways information and data can be exploited to conceal additional information.

For many years Information Hiding has captured the imagination of researchers. Digital watermarking and steganography techniques are used to address digital rights management, protect information, and conceal secrets. Information hiding techniques provide an interesting challenge for digital forensic investigations. Information can easily traverse through firewalls undetected. Research into steganalysis techniques aids in the discovery of such hidden information as well as leads research toward improved methods for hiding information. Related research themes include: anonymous communications, anonymous online transactions, covert channels in computer systems, covert/subliminal communications, detection of hidden information (steganalysis), digital forensics, information hiding aspects of privacy, steganography, subliminal channels in cryptographic protocols, watermarking for protection of intellectual property, and other applications.

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking.

Reviewing some of the requirements that are necessary to provide a useful and effective watermarking scheme. These requirements apply to any data type in general but we focus on requirements that are most useful for destination-based rather than source-based applications. The three features that they examine for our application are: transparency, robustness, and capacity. Transparency refers to the perceptual quality of the data being protected. For the case of image data, the watermark should be invisible over all image types. Such a requirement is most challenging for images composed of large smooth areas. The digital watermark should also be robust to signal processing. Ideally, the amount of signal distortion necessary to remove the watermark should degrade the desired image quality to the point of becoming commercially valueless.

Typical signal processing includes intentional transformations of the image data as well as illegal attempts to remove or transform the watermark into another valid watermark. Typical image transformations include compression, resampling, dequantization, image enhancements, cropping, and half toning. For destination-based watermarking, capacity may be a critical issue for widely distributed content. By capacity they mean the ability to be able to detect the watermarks with a low probability of error as the number of watermarks increases. The watermarking technique should provide a framework to insert the maximum number of distinguishable watermarks.

They would like to embed a digital signature into an original image that is imperceptible and is difficult to remove without destroying the original image quality. For the receiver-based problem, it may also wish to provide the maximum number of unambiguous watermarks. They argue that by using visual models, we can adapt each watermark sequence to the local properties of the image providing a watermark that is transparent and robust. As an example, they show several images where image-adaptable watermarks may not provide tremendous gains due to the fairly uniform perceptual characteristics of the original images.

Here, the watermarking techniques introduced here take advantage of the research results on developing useful visual models for image compression. Specifically, perceptual coders based on the JND paradigm are ideally suited in addressing the watermarking problem. For compression applications, the JND thresholds determine optimum quantization step sizes or bit allocations for different parts of the image as determined by a model of the human visual system and local image characteristics. In practice, the amount of side information needed to send all the threshold values is prohibitive for image compression applications. Therefore, some average threshold values are chosen based on either the most sensitive portion of an image to provide transparent image quality at variable bit rate or based on a fixed bit rate with resulting variable image quality.

At times have a prior knowledge about some of the image transformations that will be applied to the watermarked image and it is best to take advantage of this knowledge in the watermarking process. JPEG is the current international standard for color still image compression. Therefore, it is important to examine how to take advantage of visual models within this framework even though block-based DCT's are not ideal in terms of mimicking our visual system's structure. A perceptually based watermarking algorithm is also proposed based on wavelet decomposition where the threshold values have also been derived previously for image compression. Frequency sensitivity thresholds are determined for a hierarchical decomposition using the 9-7 biorthogonality filters. Due to the hierarchical decomposition, this approach has the advantage of constructing watermark components that have varying spatial support providing the benefits of both a spatially local and a spatially global watermark. The watermark component with local spatial support is suited for local visual masking effects and is robust to signal processing such as cropping. The watermark component with global spatial support is robust to operations such as low pass filtering.

Second-order statistics are regarded as critical features for visual pattern discrimination. Karhunen–Loève transform is a projection whose directions are associated with the second order statistics of the data samples. One interesting feature of the SOS metric is that it shapes the SOS watermark pattern into distinct KLT spectra from the cover image. As

aforementioned, the SOS watermark pattern exhibits the eigen values being reciprocal to the cover image's eigen values that is, the SOS watermark pattern concentrates most of its energy in the least principal components of the cover image. SOS metric is employed on Quantization Index Modulation image watermarking. To develop the QIM concept, begin by viewing the embedding function as an ensemble of functions indexed. Denote the functions in this ensemble as to emphasize this view. If the embedding-induced distortion is to be small, each function in the ensemble must be close to an identity function in some sense. That the system needs to be robust to perturbations suggests that the points in the range of one function in the ensemble should be far away in some sense from the points in the range of any other function. Quantizes are just such a class of discontinuous, approximate-identity functions. Then, QIM refers to embedding information by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantize or sequence of quantizes. Conveniently, properties of the quantizer ensemble can be related directly to the performance parameters of rate, distortion, and robustness. The design of QIM systems involves the choice of practical quantizer ensembles for such systems, which now explore.

III. PROPOSED WORK

A. Perceptual Spread Spectrum Watermarking

Focus on the watermark embedding step of spread spectrum watermarking. Without loss of generality, embed one bit of message into a cover image. The watermarked image is obtained to generate the watermark pattern, a pseudorandom carrier is first modulated by and then is weighted by watermark strength, while the key controls the generation of and ensures the security of the watermark. In principle, the watermark robustness is evaluated by the average bit error rate (BER) over a set of cover images at the decoder, yet the BER cannot be simply compared due to four factors. The factors are Watermark attack, Watermark payload, Detection threshold, Smart detector. Focus on the watermark embedding step of spread spectrum watermarking. Embed one bit of message m, , $m \in \{-1, +1\}$ into a cover image X. The watermarked image is obtained by Y=X+W ; to generate the watermark pattern W, a pseudorandom carrier P is first modulated by m and then is weighted by watermark strength, while the key k controls the generation of P and ensures the security of the watermark. Consequently, W highly correlates with mP. Denote the correlation by

$$c = \frac{m\, P^T W}{(\sigma_y^2 . q)}$$

Where σ^2 is the variance of P and is often normalized to 1. The correlation c reflects the global watermark strength. The embedding process can be expressed in the vector form.

$$Y = X + W$$

The watermarked image is possibly corrupted by attacking, which is usually modeled as additive noise.

$$Z = Y + N$$

B. Applying various attacks on the image

At the decoder, the correlation of can roughly capture the survival robustness after attacking. The absolute value of correlation usually decreases with the attack strength, and the descending trend reflects the robustness against such type of attack. In this way, avoid bothering to try all watermark payloads and the detection thresholds.
In principle, the watermark robustness is evaluated by the average bit error rate (BER) over a set of cover images at the decoder, yet the BER cannot be simply compared due to four factors.

Watermark attack - Watermark robustness is a concept closely related to the watermark attack. Different type and strength of attacks may affect the BER to different extents.

Watermark payload - The BER also depends heavily on the watermark payload. For the watermark designer, the payload setting is a compromise due to the application requirements and the channel environments.

Detection threshold - The threshold in influences the BER and the false alarm rate (i.e., reporting watermark from innocent images) in opposite way. To achieve a low BER and avoid being swapped by false alarm, the threshold setting is a Compromise for the watermark decoder.

Smart detector - The smart detecting methods, which are often based on the prior knowledge about the embedding methods, may detect watermarks more efficiently and thus improve the BER. To conclude, the robustness is a characteristic dependent on several prerequisites. It is still very challenging for the embedded to predict the BER. Resort to measure the robustness in a simple way. For the embedded who has little knowledge about the potential attacks or the smart detectors, maximizing the correlation of is an intuitive strategy to obtain a robust watermark. Actually, the BER is derived to decrease with the correlation of in assumption that the cover image and the attack noise are independent Gaussian signals. Maximizing correlation is also adopted defining the expected robustness.

$$R(X, Y; m, k) = \frac{m\, P^T W}{(\sigma_y^2 . q)}$$

C Detection Process

Implement a simple detection method, LCD, is employed. This is usually efficient in an open industrial society, where watermark decoders have little prior knowledge about watermark embedders and the

interoperability between the different spread spectrum watermarking algorithms can be supported. However, for a closed society, a more sophisticated detector associated with the watermark embedding method may improve the performance. Present a KLT-based detector associated with the SOS watermark. The detector first estimates the SOS watermark by filtering the received image and then performs the normalized LCD between the estimated watermark and the watermark carrier. One interesting feature of the SOS metric is that it shapes the SOS watermark pattern into distinct KLT spectra from the cover image. As aforementioned, the SOS watermark pattern exhibits the eigen values being reciprocal to the cover image's eigenvalues that is, the SOS watermark pattern concentrates most of its energy in the least principal components of the cover image. Therefore, it is reasonable to estimate SOS watermark pattern by "high-pass" filtering the received image in the KLT domain of the cover image. Although the KLT bases of the cover image are not available for a blind watermark detector, it is found that the SOS watermarked images have approximately equal KLT bases with those of the cover images, except that the least principal KLT bases are regrouped in order. Consequently, it is feasible to do filtering in the KLT domain of the received image. The filter shows a high-pass frequency response function as the curve marked by dots. Note that the filter is defined in the KLT domain of the received image, approximately show it in that of the cover image for illustration purpose. By the eigen decomposition of the covariance matrix of the received image samples, the decoder has $S' = U'\Delta'U'^{T}$. The columns of U'^{T} represent the KLT bases of the received image and Δ' has a^2 eigen values, in a descending order as its diagonal elements.

D . Second-Order Statistics Based Metric Method

Second-order statistics are regarded as critical features for visual pattern discrimination. Karhunen–Loève transform is a projection whose directions are associated with the second order statistics of the data samples. Along the principal directions, samples present a large variance (the second-order moment).Such directions capture the typical appearance of the samples and are often used for matching. The local variance (i.e., the luminance variance of the local image block) is another second-order statistics, which has been exhaustively studied and usually employed to capture the texture masking effect in images. SOS performs quite well, and it is the only metric which always keep its difference from the highest correlation within 0.03 for all the data sets.

E. Quantization Index Modulation method

To develop the QIM concept, begin by viewing the embedding function as an ensemble of functions indexed. Denote the functions in this ensemble as to emphasize this view. If the embedding-induced distortion is to be small, each function in the ensemble must be close to an identity function in some sense. That the system needs to be robust to perturbations suggests that the points in the range of one function in the ensemble should be far away in some sense from the points in the range of any other function. Quantizes are just such a class of discontinuous, approximate-identity functions. Then, QIM refers to embedding information by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantize or sequence of quantizes. Conveniently, properties of the quantize ensemble can be related directly to the performance parameters of rate, distortion, and robustness. The design of QIM systems involves the choice of practical quantize ensembles for such systems, which now explore. In the process, obtain additional insights into the design, performance evaluation, and implementation of QIM embedding methods, particularly those of low complexity.

F. Performance Evaluation

Finally evaluating the performance of this proposed approach for this problem in this module. Here the performance comparison of the approaches based on the following parameter is correlation and quality performance of the three types of watermarks. The experimental results show that our enhanced approach is performs better than the existing approaches. Thus it will be clear that the SOS and the PSNR value that will show that our approach will decrease the distortion and will maximize the correlation between the cover image and the carrier image. Fig.1. Shows that the comparison by spread spectrum watermarking and quantization index modulation.

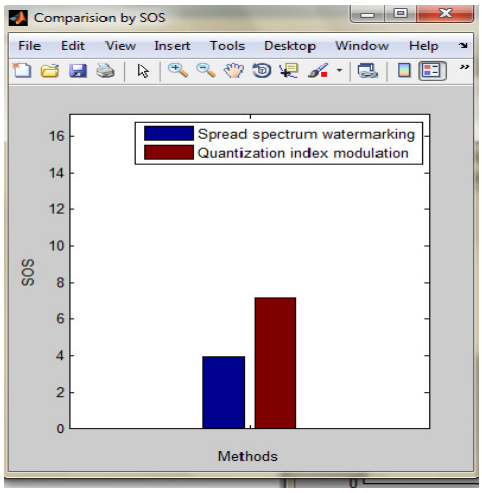

Fig.1 Comparison by SOS and QIM

IV. CONCLUSION

Focuses on implement the watermark to minimize the distortion of the watermarked image and to maximize the correlation between the watermark pattern and the spread

spectrum carrier as well as Quantization index modulation (QIM) carrier. QIM refers to embedding information by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantize or sequence of quantizes. Conveniently, properties of the quantize ensemble can be related directly to the performance parameters of rate, distortion, and robustness. The design of QIM systems involves the choice of practical quantize ensembles for such systems, which now explore. In the process, obtain additional insights into the design, performance evaluation, and implementation of QIM embedding methods, particularly those of low complexity.

REFERENCES

[1] S. Daly, "The visible differences predictor—An algorithm for the assessment of image fidelity," Human Vision, Visual Process., and Digital Display III, vol. 2666, no. 598, pp. 2–15, 2013.

[2] M. Kutter and S. Winkler, "A vision-based masking model for spread spectrum image watermarking," IEEE Trans. Image Process., vol. 11, no. 1, pp. 16–25, Jan. 2008.

[3] W. S. Lin, "Computational models for just-noticeable difference," in Digital Video Image Quality and Perceptual Coding, H. R. Wu and K. R. Rao, Eds. Boca Raton, FL: CRC, 2009.

[4] C. I. Podilchunk and W. Zeng, "Digital image watermarking using visual models," Human Vision and Electron. Imaging II, pp. 100–111, 2008.

[5] Z. Wang et al., "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2007.

[6] A. B. Watson, "DCTune: A technique for visual optimization of DCT quantization matrices for individual images," in Soc. Inf. Display Dig. Tech. Papers, 2012, vol. XXIV, pp. 946–949.

[7] H. Qi, D. Zheng, and J. Zhao, "Human visual system based adaptive digital image watermarking," Signal Process., vol. 88, no. 1, pp. 174–188, 2005.

