Wavelet based Watermarking Techniques using Principal Component Analysis Domain

U.Mehraj Ali, Research Scholar, Department of Computer Applications,
Thiagarajar College of Engineering, Madurai.
E.Vinoth Kumar, Research Scholar, Department of Computer Applications,
Thiagarajar College of Engineering, Madurai.
.A.John Sanjeev Kumar, Assistant Professor, Department of Computer Applications,
Thiagarajar College of Engineering, Madurai.

ABSTRACT
with increasing use of internet and effortless copying, tempering and distribution of digital data, copyright protection for multimedia data has become an important issue. Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. In digital watermarking an imperceptible signal “mark” is embedded into the host image, which uniquely identifies the ownership. After embedding the watermark, there should be no perceptual degradation. These watermarks should not be removable by unauthorized person and should be robust against intentional and unintentional attacks. In this paper the method of characterizing is the most important and distinguishing features of wavelet-based watermarking schemes. Copyright protection is considered and building the gained experience. It has been implemented with two distinguishing watermarking schemes. Watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital image signals and documents. The data is hidden in the message without the end user's knowledge. While the addition of the hidden message to the signal does not restrict that signal's use, it provides a mechanism to track the signal to the original owner.

Keywords
image watermarking, wavelet transform, liner filtering

1. INTRODUCTION
The main theme issued to wavelet based digital watermarking techniques that have been developed in order to help in protecting the copyright of digital images and to verify multimedia data integrity. Most watermarking techniques transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way.Image Watermarking imperceptibly embeds data into a host image. The Original Image (host image) is modified using the signature data to create the watermarked image. In this process, some error or distortion is introduced. To ensure transparency of the embedded data, the amount of image distortion due to the watermark embedding process has to be small. The watermarked image is then distributed and may circulate from legitimate to illegitimate customers. Thereby, it is subjected to various kinds of image distortion. Image distortion may result from lossy image compression, re-sampling or from specific attacks on the embedded data.

Digital watermarks are pieces of information added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. This information can be textual data about the author, its copyright, etc; or it can be an image itself. The information to be hidden is embedded by manipulating the contents of the digital data, allowing someone to identify the original owner, or in the case of illicit duplication of purchased material in which the buyer involved. These digital watermarks remain intact under transmission or transformation, allowing us to protect ownership rights in digital form.

Wavelet Based Watermarking Techniques
This section gives an overview of the numerous wavelets based digital watermarking techniques that has been developed to protect the copyright of digital images and to verify multimedia data integrity. Most watermarking techniques transform the host image into a domain that facilitates embedding of the watermark information in a robust and imperceptible way. The following principle embedding strategies that can be used to embed a watermark in a host image:

1. Linear additive embedding

i. Gaussian sequence

ii. Image fusion

2. Non-linear quantization embedding

i. Scalar quantization

ii. Vector quantization

3. Miscellaneous embedding techniques Additive embedding strategies are characterized by the linear modification of the host image and the correlative processing in the detection stage. The quantization schemes on the other hand perform non-linear modifications and detect the embedded message by quantizing the received samples to map them to the nearest reconstruction point

LL1	HL_1
LH_1	HH_1

Figure 1: DWT sub-bands.

Principal Component Analysis

Principal component analysis (PCA) has been called one of the most valuable results from applied linear algebra. PCA is used abundantly in all forms of analysis - from neuroscience to computer graphics - because it is simple, non-parametric method of extracting relevant information from confusing data sets. With minimal additional effort PCA provides a roadmap in order to explain how to reduce a complex datasets to a lower dimension, to reveal the sometimes hidden, simplified structure that often underlie it.
In this paper, we propose an imperceptible and robust image watermarking algorithm based on Discrete Wavelet Transform and Principal Component Analysis (PCA). DWT is more computationally efficient than other transform methods like DFT and DCT. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify areas in the host video frame where a watermark can be embedded imperceptibly. It is known that even after the decomposition of the image frame using the wavelet transformation there exist some amount of correlation between the wavelet coefficients.
PCA is basically used to hybridize the algorithm as it has the inherent property of removing the correlation amongst the data i.e. the wavelet coefficients and it helps in distributing the watermark bits over the sub-band used for embedding thus resulting in a more robust watermarking scheme that is resistant to almost all possible attacks. The watermark is embedded into the luminance component of the extracted frames as it is less sensitive to the Human Visual System (HVS).

2. EXISTING SYSTEM

Image Watermarking imperceptibly embeds data into a host image. The Original Image (host image) is modified using the signature data to create the watermarked image. In this process, some error or distortion is introduced. To ensure transparency of the embedded data, the amount of image distortion due to the watermark embedding process has to be small. The watermarked image is then distributed and may circulate from legitimate to illegitimate customers. Thereby, it is subjected to various kinds of image distortion. Image distortion may result from e.g. lossy image compression, re-sampling or from specific attacks on the embedded data.

3. PROPOSED SYSTEM

Digital Image Watermarking is first characterizing the most important and distinguishing features of wavelet-based watermarking schemes. The overwhelming amount of algorithms proposed in the Literature Study. Application scenario, copyright protection is considered and building on the experience that was gained, implemented two distinguishing watermarking schemes. Watermarking technology plays an important role in securing the business in which it allows that place in an imperceptible mark in the multimedia data to identify the legitimate owner, track authorized users or detect malicious tampering of the document. Conversion of an image from a frequency domain to a spatial domain to the embedded information in a reliable and robust way to achieve high performance with low cost.

4. OVERVIEW

The information of an image is based on the spatial and spectral resolution of the imaging system. The image fusion technique is required to obtain both high spatial and high spectral resolution. This paper emphasizes the assessment and systematic analysis of image fusion techniques by measuring the quantity of enhanced information in fused images. The different measuring parameters such as Entropy, Correlation Coefficient, and Mutual Information measure, Fusion Factor, Fusion Symmetry and Signal to Noise ratio along with the proposed parameter Fusion index are used for evaluating the performance of image fusion techniques.
These parameters are employed on three image fusion techniques- Principal component analysis, Multiplicative merge and Brovey transform. The results are compared with the Wavelet transform technique. The comparative study indicates that Wavelet transform fusion technique provides not only a' better look' image but also preserves the spectral information content. The parameters evaluated for various fusion techniques prove that the Wavelet transform technique surpasses the other fusion techniques.

5. MODULE DESCRIPTION

1. DWT Embedded process:

Data Embedding:
Watermarking technique embed watermarks into the DC area while preserving good quality. The gray image decomposed into several bands by wavelet transform. To embed watermark i.e. a pseudo-random binary sequence {-1,1}, a reference DC′ is prepared by taking low pass filtering to the original DC.

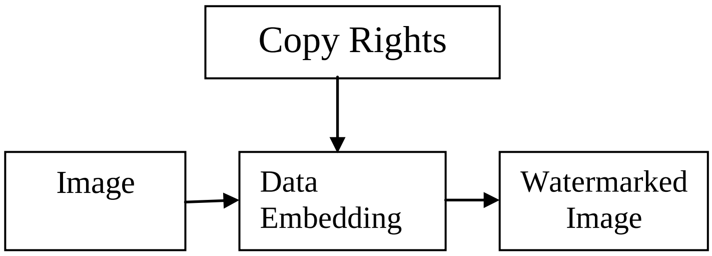

Figure 2: Image Watermarking Embedding

The DC values are changed to values smaller or larger than the DC′ values in\accordance with the corresponding watermark bits. To reduce image degradation, the watermark bits are embedded into locations with smaller differences between the DC and DC′, replaced the DC values with embedding formula LLn′ ± K×$w(i)$ …(1), where K is a factor for controlling embedding intensity and w(i) is the watermark
//Least Significant Bit (LSB)//

```
for I = 1:wm_length
if(w(i) == +1)
if(LLn(idx(i)) < LLn' (idx(i)) + K)
LLn(idx(i)) = LLn' (idx(i)) + K
end
else if(w(i) == –1)
if(LLn(idx(i)) > LLn' (idx(i)) – K)
LLn(idx(i)) = LLn' (idx(i)) – K
end
end
end (1)
```

2. Extraction:
For extraction an original image is required to extract the present watermarks. Such an extraction is classified as non-blind watermarking. The same wavelet decomposition is applied to both the original and embeddedimages. The

watermark-embedding locations are obtained from the original image. Since LLn and LLn' are obtained from the watermark embedded image, the watermarks are extracted by comparing the two values, LLn and LLn'. Then the extracted watermarks are compared with the original watermarks generated by the user key. In this comparison, used the similarity measure given, where '.' denotes the inner product.

3. Compression:

Encoding:

Image compression may be lossy where information is lost during the compression process. These schemes exploit limitations of an human visual system. Some errors are undetectable by the human eye. Even though two images are different at the bit by bit level, the human viewer cannot distinguish them. Some errors are detectable by the human eye but acceptable. Some errors are detectable and very annoying. The widely used JPEG image compression standard is a lossy compression scheme.

Decoding:

Within lossy image and video compression, a compression scheme may be perceptually lossless, in which case the human viewer cannot distinguish between the original image or video and the decompressed compressed image or video which has errors introduced by the lossy compression. Most lossy image and video compression have some sort of quality factor or factors. If the quality is good enough, then the image will be perceptually lossless.

6. PRINCIPAL COMPONENT ANALYSIS:

Principal component analysis (PCA) is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of uncorrelated variables called principal components. The number of principal components is less than or equal to the number of original variables. PCA is a method of identifying patterns in data, and expressing the data in such a way so as to highlight their similarities and differences. Since patterns in data can be hard to find in data of high dimension, where the advantage of graphical representation is not available, PCA is a powerful tool for analyzing data.

The other main advantage of PCA is that once these patterns in the data have been identified, the data can be compressed by reducing the number of dimensions, without much loss of information. It plots the data into a new coordinate system where the data with maximum covariance are plotted together and is known as the first principal component. Similarly, there are the second and third principal components and so on.

The maximum energy concentration lies in the first principal component. The following block diagram shows the embedding and extraction procedure of the watermark. In the proposed method the binary watermark is embedded into each of the video frames by the decomposition of the frames into DWT sub bands followed by the application of block based PCA on the sub-blocks of the low frequency sub-band. The watermark is embedded into the principal components of the sub-blocks. The extracted watermark is obtained through a similar procedure.

Algorithms for watermarking using DWT AND PCA:

Algorithm 1:

a) Embedding Procedure

Step 1: Convert the n × n binary watermark logo into a vector W = { w1, w2 , ……, wn × n } of '0's and '1's.

Step 2: Divide the video (2N × 2N) into distinct frames.

Step 3: Convert each frame from RGB to YUV color format.

Step 4: Apply 1-level DWT to the luminance (Y component) of each video frame to obtain four sub-bands LL, LH, HL and HH of size N x N .

Step 5: Divide the LL sub-band into k non-overlapping sub-blocks each of dimension n × n (of the same size as the watermark logo).

Step 6: The watermark bits are embedded with strength α into each sub-block by first obtaining the principal component scores by Algorithm 2. The embedding is carried out as equation 1.

$$\text{Score}'_i = \text{Score}_i + \alpha W \qquad (1.1)$$

Where Score $_i$ represents the principal component matrix of the i^h sub-block.

Step 7: Apply inverse PCA on the modified PCA components of the sub-blocks of the LL sub-band to obtain the modified wavelet coefficients.

Step 8: Apply inverse DWT to obtain the watermarked luminance component of the frame. Then convert the video frame back to its RGB components.

b) Extraction Procedure

Step 1: Divide the watermarked (and possibly attacked) video into distinct frames and convert them from RGB to YUV format.

Step 2: Choose the luminance (Y) component of a frame and apply the DWT to decompose the Y component into the four sub-bands LL , HL , LH , and HH of size N×N.

Step 3: Divide the LL sub-band into n × n non overlapping sub-blocks.

Step 4: Apply PCA to each block in the chosen sub band LL by using Algorithm 2.

Step 5: From the LL sub-band, the watermark bits are extracted from the principal components of each sub-block as in equation 2.

$$W_i = \frac{(Score'_i - Score_i)}{\alpha} \qquad (1.2)$$

Where W'_i is the watermark extracted from the i^{th} sub block.

Algorithm 2:

The LL sub-band coefficients are transformed into a new coordinate set by calculating the principal components of each sub-block (size n x n).

Step 1: Each sub-block is converted into a row vector D_i with n2 elements (i=1,2…k).

Step 2: Compute the mean μ_i and σ_i standard deviation of the elements of vector D_i.

Step 3: Compute according to the following equation

$$Z_i = \frac{(D_i - \mu_i)}{\sigma_i} \qquad (1.3)$$

Here Z_i represents a centered, scaled version of D_i, of the same size as that of D_i

Step 4: Carry out principal component analysis on Z_i (size 1 x n^2) to obtain the principal component coefficient matrix coeffi (size $n^2 \times n^2$).

Step 5: Calculate Vector $score_i$ as

$$score_i = Z_i \times coeff_i$$

Where $score_i$ represents the principal component scores of the i^{th} sub-block.

Principal Component Analysis Diagram:

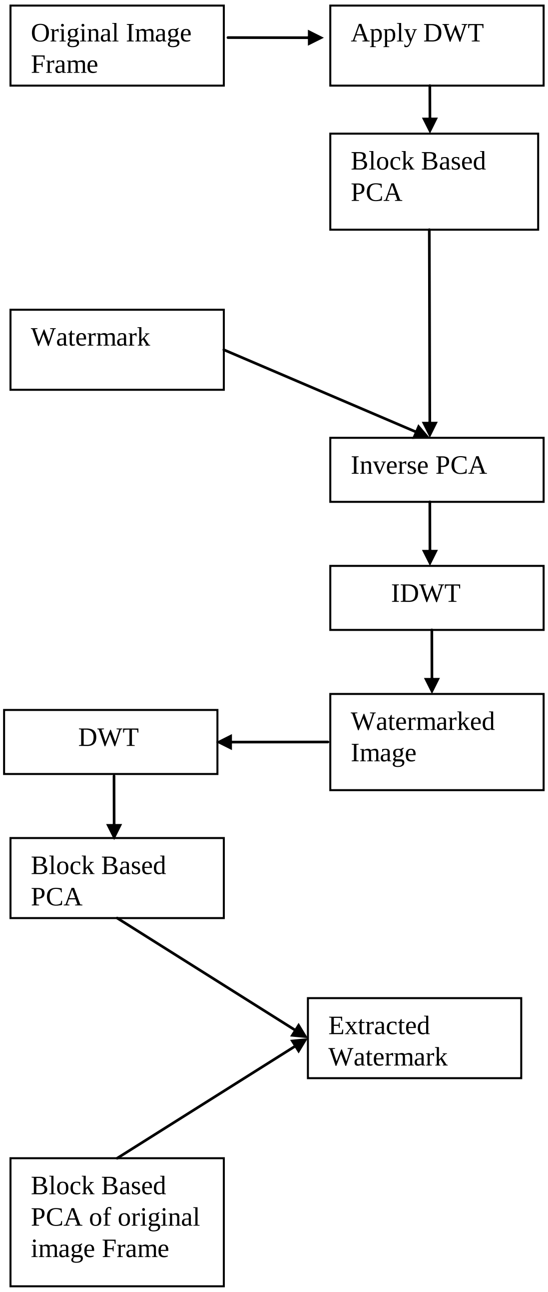

Figure 3: Principal Component Analysis Diagram

Figure 4: (a) Original watermark

Figure 4: Extracted binary watermark

I. SCREEN SHOTS

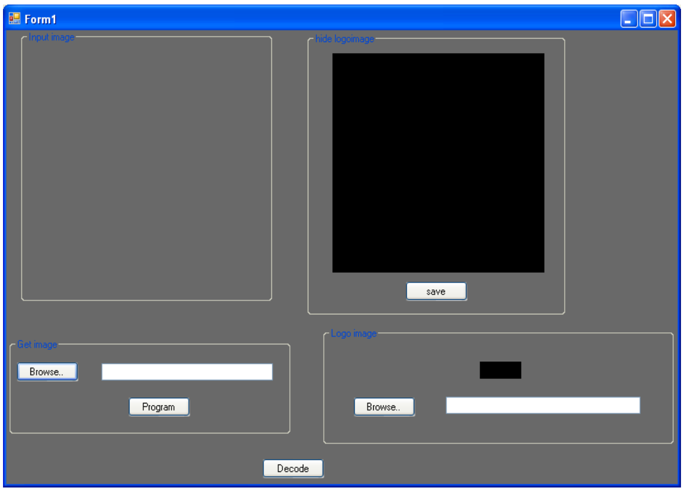

Figure 5: Initial Process

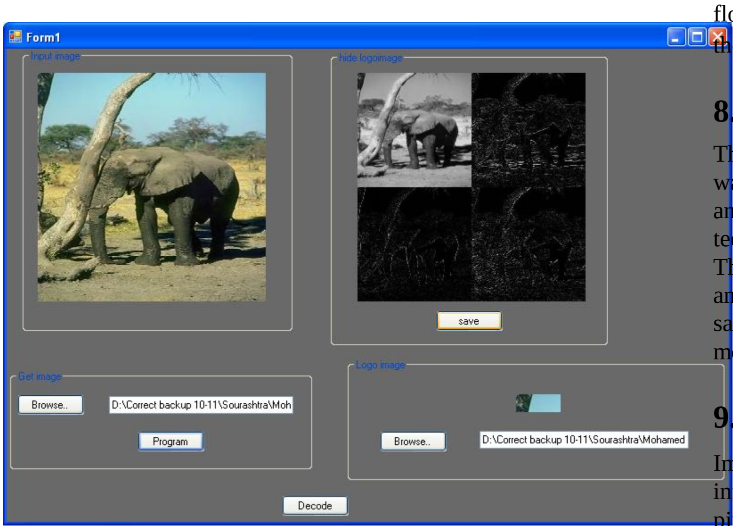

Figure 6: Intermediate Process

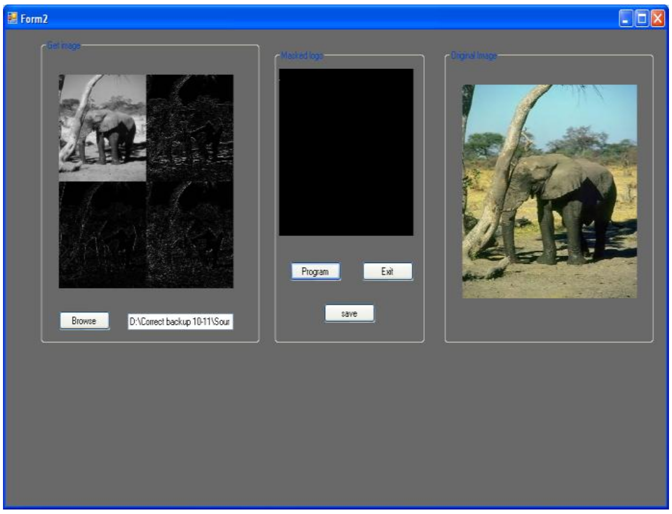

Figure 7: Final Process

7. RESULT AND DESCRIPTION

The Screen has been put upon here with three levels saying Initial Process, Intermediate Process and the Final Process. In the Figure 5 the picture is demonstrating the way of giving the input to be watermarked. The Figure 6 shows the picture and the space allocated to be watermarked. Figure 7 shows the destination point of the paper. This has been implemented using a software toolkit and thus the destination has been reached.

The image submission shows the image created using system on a variety of scene. The system is strongly encouraged to view the image as it was generated. The effects are hard to show in the paper. This system was implemented on an Intel Core 2 duo, Processor 2.93GHz, 4GB DDR2 RAM and 1 Network Interface Card (NIC). However, refining the optical flow takes a lot of time distribution, the time depending on the sizes of the image or the file we use.

8. CONCLUSION

The review of the various watermarking techniques in the wavelet transform domain. The two simulated techniques are analyzed in the robustness for copyright scenario. Both the techniques were found non-obtrusive in gray level images. Then the extracted watermarks from the noisy images are in an acceptable degree of correlation technique. Therefore, the say technique has copied the added noise degradation and is more robust for such standard attacks

9. FUTURE ENHANCEMENTS

Image watermarking is the process of inserting hidden information in an image by introducing modifications to its pixels with the expectation of minimum perceptual disturbance. Watermarking is robust but still these could be the possible sources of attacks:

- Enhancement: sharpening, contrast, color correction
- Additive and multiplicative noise: Gaussian, uniform, speckle
- Linear filtering: low pass, high pass, band pass
- Nonlinear filtering: median filters, rank filters, morphological filters

10. REFERENCES

[1] S.Sinha,S.Pramanick,A. Jagatramka,P. Bardhan,D.K. Kole,A. Chakraborty, "Digital Video Watermarking using Singular Value Decomposition", Proceedings on IEEE EDS Student Paper Conference, pp. 53-56, 2011.

[2] M.K.Thakur, V. Saxena, J. P.Gupta, "A Performance Analysis of Objective Video Quality Metrics for Digital Video Watermarking," Computer Science and Information Technology (ICCSIT), 2010, 3rd IEEE International Conference ,Vol. 4, pp. 12- 17,2010.

[3] Datta,K.;Sengupta,I.; Sch. of Inf. Technol., Indian Inst. of Technol., Kharagpur, India Communication Software and Networks, 2010. ICCSN '10. Second International Conference on Issue Date: 26-28 Feb. 2010

[4] M.Natarajan G. Makhdumi1,"Safeguarding the Digital Contents: Digital Watermarking," DESIDOC Journal of Library & Information Technology, Vol. 29, May 2009, pp. 29-35.

[5] F.Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Processing, 1998,vol. 66, no. 3,pp.283-301. [9] T. Khatib, A. Haj, L. Rajab, H. Mohammed, " A Robust Video Watermarking Algorithm", Journal of Computer Science, vol. 4, pp. 910-915, 2008.

[6] T.Tokar, T. Kanocz, D. Levicky, "Digital watermarking of uncompressed video in spatial domain," 9th International Conference on Radioelectronica, IEEE, pp. 319-322, 2009.

[7] T.D. Hien, Y.W. Chen, Z. Nakao, "PCA Based Digital Watermarking", KES 2003, LNAI 2773, pp. 1427-1434, 2003.

[8] S.A.K. Mostafa, A.S. Tolba, F. M. Abdelkader, H.M. Elhindy, "Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform," IJCSNS International Journal of Computer Science and Network Security, vol.9, No.8, August 2009.

[9] T. Khatib, A. Haj, L. Rajab, H. Mohammed, " A Robust Video Watermarking Algorithm", Journal of Computer Science, vol. 4, pp. 910-915, 2008.

[10] S.Sinha, S. Pramanick, A. Jagatramka,P. Bardhan,D.K. Kole,A.Chakraborty, "Digital Video Watermarking using Singular Value Decomposition", Proceedings on IEEE EDS Student Paper Conference, pp. 53-56, 2011. [19] A-Haj and T. Manasrah, "Non-Invertible Copyright Protection of Digital Images Using DWT and SVD," Digital Information Management, 2007, ICDIM '07, 2nd International Conference ,vol. 1, pp. 448 – 453, 2007.

[11] Kang, WenjunZeng , J. Huang, "A Multi-band Wavelet Watermarking Scheme" , International Journal of Network Security ,vol 6 ,no 2, pp. 121–126, Mar 2008. [21] T. Hu, J. Wei, "A digital video watermarking scheme based on 1D-DWT", IEEE, International Conference on Biomedical Engineering and Computer Science , 2010, pp. 1-3.

[12] Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi, "A New Robust Watermarking Embedding into Wavelet DC Components", ETRI Journal, Volume 24, No. 5, October 2002.

[13] Langelaar, G.C., Setyawan, I., Lagendijik, R.I., 2000. Watermarking digital image and video data. IEEE signal Process. Magazine (September), 20-46.

[14] Y. R. Lin, H.Y. Huang and W.H Hsu, "An embedded watermark technique in video for copyright protection", IEEE,18th International Conference on Pattern Recognition , vol 00., pp. 795- 798, 2006.

[15] S. Voloshynovskiy, S. Pereira, T. Pun, "Watermark attacks," Erlangen Watermarking Workshop 99, October 1999. [7] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State of - Art Overview," IEEE Signal Processing Magazine, vol. , pp. 20-46, Sep. 2000.