DCT-BASED DIGITAL IMAGE WATERMARKING VIA IMAGE SEGMENTATION TECHNIQUES

Abstract: In recent years, digital watermarking techniques have been proposed to protect the copyright of multimedia data. Different watermarking schemes have been suggested for images. This paper proposes a watermarking algorithm based on image segmentation and discrete cosine transform (DCT). The image is first segmented using expectation maximization (EM) algorithm. For each segment, the image segment is subdivided into pixels blocks of size 8× 8 (64pixels), and zigzag reordered. The DCT of the block is then computed. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment. Different experiments are conducted to show the performance of the scheme under different types of attacks. The results show that our proposed watermark scheme is robust to common signal distortions, including geometric manipulations.

Keywords: Discrete cosine transform (DCT), digital watermarking, image segmentation

1. INTRODUCTION

Most watermarking research and publications are focused on digital images. The reason might be that there is a large demand for image watermarking products due to the fact that there are so many images available at no cost on the World Wide Web which need to be protected. Meanwhile, the number of image watermarking publications is too large. However, most techniques share common principles. The watermark signal is typically a pseudorandom signal with low amplitude, compared to the image amplitude, and usually with spatial distribution of one information (i.e., watermark) bit over many pixels.

A lot of watermarking methods are in fact very similar and differ only in parts or single aspects of the three topics, signal design; embedding; and recovery. The information that is embedded is usually not important for the watermarking itself. However, there are methods that are designed to embed and extract one out of a codebook of codes, and thus cannot accommodate arbitrary information. Other proposed schemes modulate the codes available in the codebook with arbitrary information bits and can thus accommodate arbitrary messages.

The watermark signal is often designed as a white or colored pseudorandom signal with, e.g., Gaussian, uniform or bipolar probability density function. In order to avoid visibility of the embedded watermark, an implicit or explicit spatial or spectral shaping is often applied with the goal to attenuate the watermark in areas of the image where it would otherwise become visible. The resulting watermark signal is sometimes sparse and leaves image pixels unchanged, but mostly it is dense and alters all pixels of the image to be watermarked. The watermark signal is often designed in the spatial domain [1],[2],[3],[4],[5] and [6], but sometimes also in a transform domain like the full-image discrete cosine transform (DCT) domain, block-wise DCT domain [7], [8],[9],[10] and discrete wavelet transform (DWT) [11],[12].

The signal embedding is done by addition or signal-adaptive (i.e., scaled) addition, mostly to the luminance channel alone, but sometimes also to color channels, or only to color channels. The addition can take place in the spatial domain, or in transform domains such as the discrete Fourier transform (DFT) domain, the full-image DCT domain, the block-wise DCT domain [7],[8],[9], the wavelet domain [11],[12], the fractal domain, the Hadamard domain, the Fourier–Mellin domain, or the Radon domain. It is often claimed that embedding in the transform (mostly DCT or wavelet) domain is advantageous in terms of visibility and security.

The main contribution of this paper is to present a new watermarking scheme that is based on expectation maximization (EM) segmentation algorithm and discrete cosine transform (DCT). Section 2 presents the main requirements and applications of watermarking. Section 3 discusses the image segmentation techniques. The proposed watermarking scheme is presented in Section 4. This is followed by the experiment results in Section 5. Finally, the conclusions are presented in Section 6.

2. IMAGE WATERMARKING REQUIREMENTS AND APPLICATIONS

Each watermarking application has its own specific requirements. Therefore, there is no set of requirements to be met by all watermarking techniques.

Perceptual Transparency: In most applications the watermarking algorithm must embed the watermark such that this does not affect the quality of the underlying host data. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark. Even the smallest modification in the host data may become apparent, however, when the original data is compared directly with the watermarked data. Since users of watermarked data normally do not have access to the original data, they cannot perform this comparison. Therefore, it may be sufficient that the modifications in the watermarked data go unnoticed as long as the data are not compared with the original data.

Robustness: It is desirable that the watermark always remains in the host data, even if the quality of the host data is degraded. Examples of degradations are lossy compression techniques, filtering, re-sampling, digital-analog (D/A) and analog-digital (A/D) conversion.

There are many applications for watermarking including copyright protection, fingerprinting, copy protection, broadcast monitoring, data authentication, indexing, medical safety, and data hiding.

There are three main issues in the design of a watermarking system [1]:

- Design of the watermark signal to be added to the host signal. Typically, the watermark signal depends on a key and watermark information.
- Design of the embedding method itself that incorporates the watermark signal into the host data yielding watermarked data.

• Design of the corresponding extraction method that recovers the watermark information from the signal mixture using the key and with help of the original or without the original

The first two issues, watermark signal design and watermark signal embedding, are often regarded as one, specifically for methods were the embedded watermark is host signal adaptive.

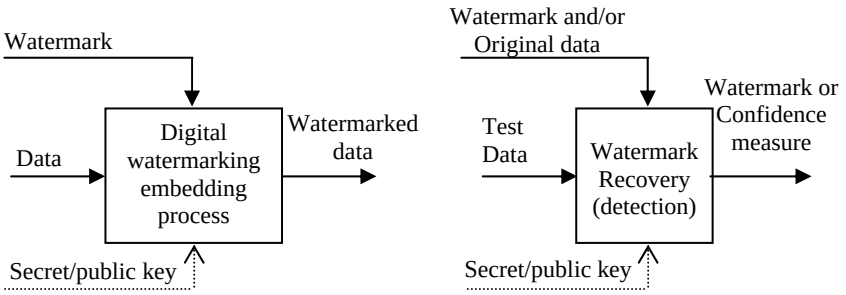


Figure 1. Digital watermarking embedding and detecting systems

Figure 1 illustrates the concept. Figure 1(a) shows the generic watermarking scheme for the embedding process. The input to the scheme is the watermark, the host data, and an optional public or secret key. The host data may, depending on the application, be uncompressed or compressed, however, most proposed methods work on uncompressed data. The watermark can be of any nature, such as numbers, text, or an image. The generic watermark recovery process is depicted in Figure 1(b). Inputs to the scheme are the watermarked data, the secret or public key, and, depending on the method, the original data and the original watermark. The output of the watermark recovery process is either the recovered watermark or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

3. IMAGE SEGMENTATION TECHNIQUES

A central problem, called *segmentation*, is used originally to distinguish objects from background or objects from each other. For intensity images (i.e., those represented by point-wise intensity levels) four popular approaches are: threshold techniques, edge-based methods, region-based techniques, and connectivity-preserving relaxation methods.

Segmentation algorithms also include expectation-maximization algorithm [13], K-means algorithm [14], and other clustering techniques such as QT clustering algorithm and Fuzzy *c*-means clustering algorithm. In statistical computing, the expectation-maximization (EM) algorithm [13] is an algorithm for finding maximum likelihood estimates of parameters in probabilistic models, where the model depends on unobserved latent variables. EM is frequently used for data clustering in machine learning and computer vision. EM alternates between performing an expectation step, which computes an expectation of the likelihood by including the latent variables as if they were observed, and a maximization step, which computes the maximum likelihood estimates of the parameters by maximizing the expected likelihood found on the expectation step. The parameters found on the maximization step are then used to begin another expectation step, and the process is repeated.

The K-means algorithm [14] is an algorithm to cluster objects based on attributes into k partitions. It is a variant of the expectation-maximization algorithm in which the goal is to determine the *k* means of data generated from gaussian distributions. It assumes that the object attributes form a vector space. The objective it tries to achieve is to minimize total intra-cluster variance. The algorithm starts by partitioning the input points into k initial sets, either at random or using some heuristic data. It then calculates the mean point, or centroid, of each set. It constructs a new partition by associating each point with the closest centroid. Then the centroids are recalculated for the new clusters, and algorithm repeated by alternate application of these two steps until convergence, which is obtained when the points no longer switch clusters (or alternatively centroids are no longer changed). The algorithm has remained extremely popular because it converges extremely quickly in practice. In fact, many have observed that the number of iterations is typically much less than the number of points.

4. PROPOSED DCT-BASED IMAGE WATERMARKING VIA IMAGE SEGMENTATION TECHNIQUES

Inspired by some of the ideas proposed by Cox *et al.* [7] and the algorithm in [8], we have constructed our algorithm. In [8] their algorithm rather than embedding the watermark globally in the host image as the Cox algorithm, the original image is first segmented based on Voronoi diagram and the feature extraction points.

Our proposed algorithm is based on image segmentation and discrete cosine transform. The image is first segmented using

expectation maximization segmentation algorithm, and then each segment is divided into 8×8 blocks (64 pixels). A zigzag reordering is applied to each block of each segment (see Figure 2).

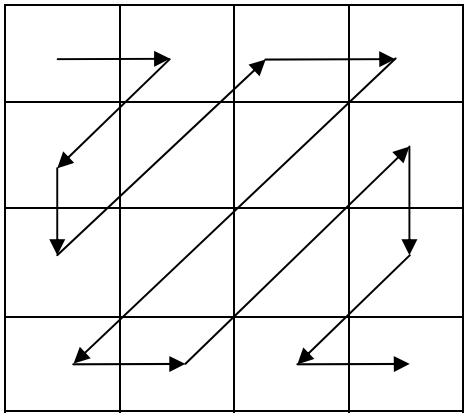


Figure 2. Zigzag reordering algorithm.

For each 8×8 block in the segments a two dimensional discrete cosine transform (2D-DCT) is applied. The DCT coefficients of each segment are then selected to be modified by the watermark in which we embed a pseudorandom sequence of real numbers in the DCT coefficients of each segment of the host image. This will boost the watermark robustness with affecting the invisibility. The embedding of the watermark is applied to each segment of the image.

To get the watermarked image, the reverse process is applied in which the two-dimensional inverse discrete cosine transform (2D-IDCT) is preformed on each 8×8 block of each segment. Each 8×8 block is reordered using dezigzag reordering which is the inverse of the zigzag reordering mentioned above. Finally the segments are merged together to form the watermarked image.

The two dimensional DCT used in our algorithm is given by

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N}, \qquad (1)$$

for $0 \le u \le M-1$, $0 \le v \le N-1$ and

$$\alpha_u = \begin{cases} 1/\sqrt{M}, & u = 0 \\ \sqrt{2/M}, & 1 \le u \le M-1 \end{cases}, \quad \alpha_v = \begin{cases} 1/\sqrt{N}, & v = 0 \\ \sqrt{2/N}, & 1 \le v \le N-1 \end{cases} \qquad (2)$$

The two dimensional IDCT is given by

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v C(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N}, \qquad (3)$$

for $0\le x\le M-1$, $0\le y\le N-1$ and α_u, α_v as defined above.

The selected DCT coefficients to be watermarked $C=\{c_1,c_2,...,c_N\}$ are modified by the watermark $W=\{w_1,w_2,...,w_N\}$ which consists of a sequence of randomly generated real numbers. These numbers have a normal distribution with zero mean and unity variance.
The modification (embedding process) is applied according to

$$c_i^{/}=c_i+\alpha\, c_i w_i \qquad (4)$$

A value of α = 1 is used in our proposed algorithm, which is shown to be empirical value of α [7],[8]. To tune the watermark energy α can be changed. The length of watermark embedded in each segment is about 1000 divided by the number of segments.
By denoting the original image by I and the watermarked image – possible distorted– by I_w , then a possibly corrupted watermark W^* can be extracted. For extraction process similar procedure as explained above is considered evolving both the original image I and the watermarked image I_w .
For evaluating the similarity of watermarks, It is highly unlikely that the extracted watermark W^* will be identical to the original watermark W . The similarity between W and W^* can be measured by

$$sim(W,W^*)=\frac{W\cdot W^*}{\sqrt{W^*\cdot W^*}}, \qquad (5)$$

as in [7]. It is obvious that the value calculated from equation (7) may change depending on the length of the watermarking vector. A normalized similarity measure can be given by

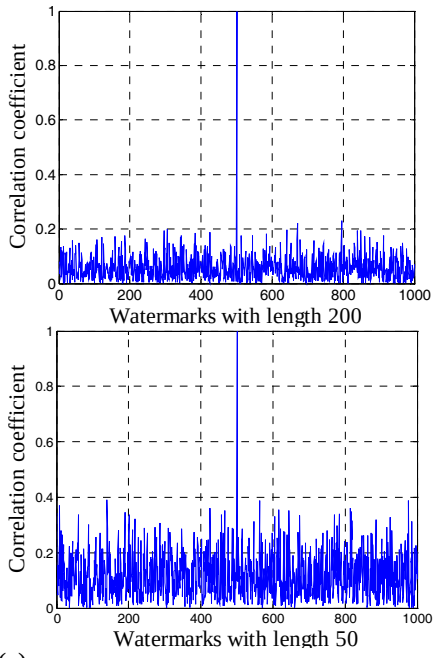
$$sim_{normalized}(W,W^*)=\frac{W\cdot W^*}{\sqrt{W^*\cdot W^*}}\Big/\frac{W\cdot W}{\sqrt{W\cdot W}}. \qquad (6)$$

Other measures are possible, including standard correlation coefficient.

5. SIMULATION RESULTS

In order to verify that the watermark detector response achieves very low false positive or negative rates, 1000 watermarks were randomly

generated with length 200. One of them is embedded on host image and then extracted and then the standard correlation coefficient is calculated for it with each of the 1000 watermarks. The result is shown in Figure 3(a) which the maximum value is achieved when the correlation coefficient is between the extracted watermark and itself before embedding. The same process was repeated with 1000 watermark of length 50, and the result is shown in Figure 3(b). It is obvious that the longer the watermark the accurate the result. Figure 4 shows original images of "Cameraman" and "Lena" and their watermarked images to demonstrate that the watermark is invisible.



(a) (b)

Figure 3. Correlation coefficient of the extracted watermark with a group of 1000 watermarks, the extracted was originally one of them.

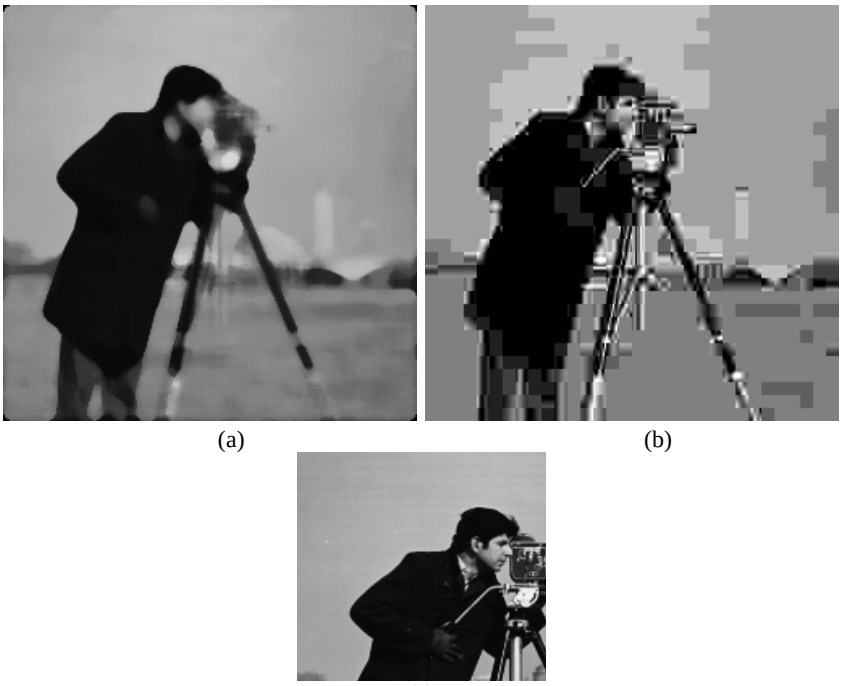
To examine our algorithm robustness, the watermarked images are exposed to common image processing operations including the geometric manipulations. The results of median filtering, JPEG compression and cropping are discussed. Also, a comparison with Cox algorithm [7] and the algorithm in [8] is provided. In the median filtering, the value of an output pixel is determined by the median of the neighborhood pixels. Median filtering is able to remove the outliers in the image without reducing the sharpness of the image. Figure 5(a)

shows the results for the median filtering of size 9×9. The results show that the robustness of our system still good even with larger sizes of the filters. This is shown in Figure 6, where the effect of image filtering on watermark detection as the output of correlation coefficient versus the filter size is displayed. Also, this figure shows that our proposed scheme outperform the one in [7] and most of [8]. To test the

Figure 4. "Cameraman" and "Lena" images and their watermarked images.

robustness against compression, the watermarked images are exposed to JPEG for different compression ratios. The watermarked image exposed to JPEG of compression ratio from 1:45 is shown in Figure 5(b). The resulting compressed image shows visible blocking artifacts as displayed in Figure 5(b). The correlation coefficients of the watermarking detector after compression using JPEG is presented in Figure 7. The JPEG compression attack results in compression ratios

ranging from 1:1 (no compression) to 45:1. This is clear form Figure 7 which reveals that the robustness declines as the watermarked image is compressed more. However, the proposed system robustness at ratio 45:1 is better than the algorithms in [7], [8], and is decaying slowly.
Applying cropping to watermarked image, a remaining 60% percentage of the watermarked image is displayed in Figure 5(c). As long as there exist a segment of the image segments in the remaining part of the image after cropping the watermark in this segment can be completely recovered even if a part of it is missing it can be partially recovered. This is because the watermark is inserted in each watermark segment as explained.



(a) (b)

(c)

Figure 5 .Watermarked image after different severe image processing attacks
a) passing it through median filter of size 9×9, b) applying jpeg compression with compression ratio 45:1, and c) remaining part of the image after cropping it by 60%

6. CONCLUSION

To conclude, we have presented a new robust watermarking scheme. The results of experiments show that this approach is very promising, because it is robust to common image processing distortions. Our

proposed system outperforms the one in [7], and at some point outperforms the one in [8] or came close to it. For the compression attacks, it is found that the robustness against JPEG compression is achieved for a compression ratio of up to 45. Moreover, robustness against average, median and Wiener filters is shown for the 3×3 up to

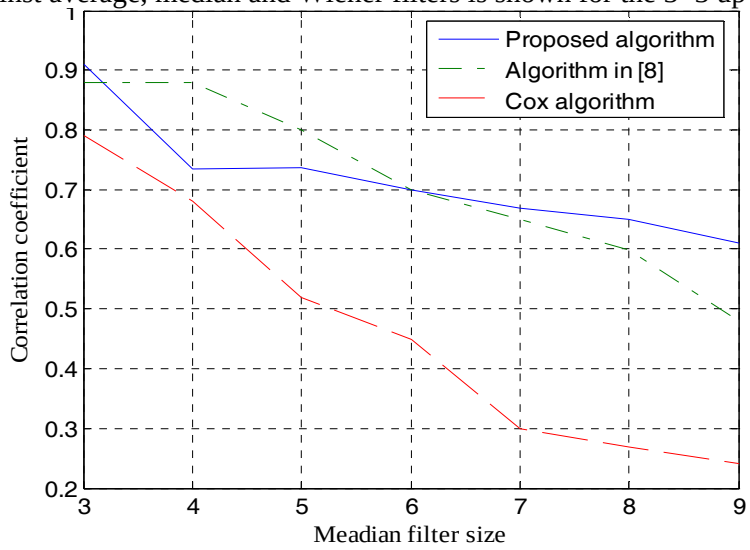


Figure 6. Correlation output of watermark detector for different Median filter size.

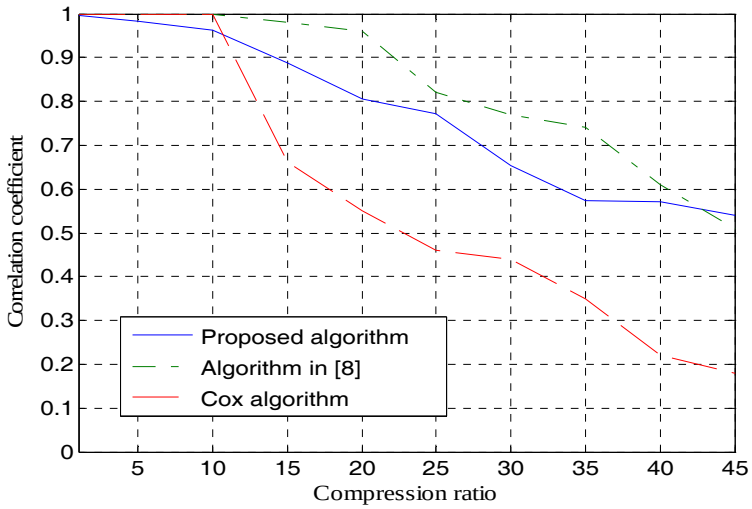


Figure 7. Correlation output of watermark detector for successive compression ratios from 5 to 45 using JPEG.

9×9-pixel neighborhood. Also, the proposed system is inherently resistant to geometric manipulation. It is observed that robustness against cropping was achieved when the watermarked image size is cropped down to 0.4 of its original size. Finally, we have shown that cropping attack is not effective in destroying the watermark.

REFERENCES

[1] F. Hartung, M. Kutter, "Multimedia watermarking techniques" *Proceedings of the IEEE*, vol. 87, issue 7, pp. 1079-1107, Jul 1999.

[2] D. P. Mukherjee, S. Maitra, and S. T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication" *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 1-15, Feb. 2004

[3] Z. Lu,D. Xu, and S. Sun, " Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization" *IEEE Trans Image Processing*, vol. 14, no. 6, pp. 822 -831, June 2005.

[4] J-B. Zheng, D. D. Feng, and R-C. Zhao, "A Multi-Channel Framework for Image Watermarking", *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics*, Guangzhou, 18-21 August 2005.

[5] P. Dong, *et al.*, "Digital Watermarking Robust to Geometric Distortions", *IEEE Transactions on Image Processing*, vol. 14, no. 12, Dec. 2005.

[6] W. Xing, Z. Lu, And H. Wang, "A Digital Watermarking Method Based on Classified Labeled-Bisecting-K-Means Clustering", *Proceedings of The 2nd Inter. Conf. Machine Learning & Cybernetics*, pp.2891-2895, Nov. 2003.

[7] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[8] M. A. Suhail and M. S. Obaidat," Digital Watermarking-based DCT and jpeg Model" *IEEE Trans. on Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640-1647, Oct. 2003.

[9] J. R. Hernández, M. Amado, and F. Pérez-González, " DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", *IEEE Tran. Image Processing*, vol. 9, pp. 55-68, Jan. 2000.

[10] Q. Cheng, and T. S. Huang, "Robust Optimum Detection of Transform Domain Multiplicative Watermarks" *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 906-924, April 2003.

[11] J. R. Kim and Y. S. Moon, "A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding" *Proceedings of the 1999 International Conf. on Image Processing* (ICIP '99), Kobe, Japan, pp. 226-230, Oct. 1999.

[12] A. Miyazaki, "On the Evaluation of Wavelet Filter Banks for Wavelet-based Image Watermarking", *Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis* pp.877-882 (2003)

[13] Arthur Dempster, Nan Laird, and Donald Rubin. "Maximum Likelihood from Incomplete Data via the EM Algorithm". *Journal of the Royal Statistical Society*, Series B, 39(1):1–38, 1977.

[14] J. B. MacQueen, "Some Methods for Classification and Analysis of Multivariate Observations", *Proceedings of 5-th Berkeley Symposium on Mathematical Statistics and Probability*, Berkeley, University of California Press, 1:281-297, 1967.