

文章编号:1001-9081(2005)02-0386-04

一种图像水印鲁棒性的协同序参量评价方法

陈永强^{1,2}, 胡汉平¹, 李新天¹

(1. 华中科技大学 图像识别与人工智能研究所, 湖北 武汉 430074;

2. 武汉工业学院 计算机与信息工程系, 湖北 武汉 430023)

(chenyqwh@hotmail.com)

摘要:针对图像水印的鲁棒性,运用协同序参量理论,提出一种基于协同序参量的定量评价方法。对载体图像完成各类鲁棒性实验,计算比较了各模式的协同序参量初始值,使用序参量演化曲线进行验证,得到相应的鲁棒性定量评价。评价结果与相关系数法一致,但更加方便和实用。

关键词:图像水印;鲁棒性;序参量;协同学

中图分类号: TP391; TP309.2 **文献标识码:** A

Image watermark robustness evaluative method based on synergetic order parameter

CHEN Yong-qiang^{1,2}, HU Han-ping¹, LI Xing-tian¹

(1. Institute of Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan Hubei 430074, China;

2. Department of Computer and Information, Wuhan Polytechnic University, Wuhan Hubei 430023, China)

Abstract: Aimed at image watermark robustness, an evaluative method based on synergetic order parameter and its usage was first advanced. Many kinds of robust experiment of Image carrier were done. After procession, the synergetic original order parameter of patterns in the set were calculated and compared. Through validation by the order parameter evolution curves, their robust conclusions were gotten. This method is more convenient and applied than the correlative coefficient method, although the two methods have same conclusion.

Key words: image watermark; robustness; order parameter; synergetics

0 引言

由于数字图像的广泛使用,图像水印是目前研究最为充分的数字水印技术。

图像水印应具有可证明性、不可感知性、鲁棒性和安全性等基本特性。鲁棒性是指在经过常规的信号处理操作后,仍能够检测到水印的能力^[1]。要求图像水印能够承受常规的操作,包括图像压缩、滤波、噪声污染、几何失真等。

水印是否具有鲁棒性,目前是使用相关性分析的判断方法。给定一个固定阈值,计算经过一定类型的操作后图像的某一相关性度量值,如大于阈值,认为可检测和提取水印,水印对此操作具有鲁棒性,反之则没有鲁棒性。使用此方法具有两个缺点,一是阈值是根据实验的结果,由经验所确定。二是可能出现两个完全不同的图像具有相同或相近的相关性度量值。有鉴于此,本文运用协同计算机的序参量理论,通过计算图像模式向量的初始序参量方法,可定量评价图像水印的鲁棒性。

1 协同序参量

1.1 序参量方程

收稿日期:2004-07-28;修订日期:2004-12-10

作者简介:陈永强(1967-),男,湖北武汉人,讲师,博士研究生,主要研究方向:网络信息安全与智能系统、数字图像处理; 胡汉平(1960-),男,湖北武汉人,教授,博士生导师,主要研究方向:智能信息安全系统; 李新天(1978-),男,湖北黄冈人,硕士研究生,主要研究方向:智能信息安全系统。

在平衡相变理论中,序参量是用于表征相变后系统的有序性质和程度。序参量的梯度动力学方程,描述了系统离开平衡点时的动力学过程。在相变前的旧结构下,序参量为0,从相变点起,序参量取非零值。

协同学研究系统的各个个体是如何进行协作,通过协同导致新的空间结构、时间结构或功能结构的形成。协同学引入了平衡相变理论中的序参量概念,并运用于协同计算机的模式识别标准模型里^[2]。

假设原型模式数为 M ,原型模式向量的维数为 N ,要求 $M \leq N$,待识别模式 q 的动态过程满足协同演化动力学方程:

$$\dot{q} = \sum_k \lambda_k v_k (v_k^* q) - B \sum_{k \neq k'} (v_k^* q)^2 (v_{k'}^* q) v_k - C(q^* q)q + F(t) \quad (1)$$

其中, q 是以输入模式 q_0 为初始值的状态向量,为待识别的试验模式向量,可分解为原型向量 v_k 和剩余量 w , $q = \sum_{k=1}^M \xi_k v_k + w$,且 $v_k^* w = 0$, q^* 为 q 的伴随向量; λ_k 为注意参数,只有当它为正的时候,模式才能被识别; $F(t)$ 为涨落力,可忽略不计; B 和 C 为指定系数,且都大于0; v_k 为原型模式向量, $v_k = (v_{k1}, v_{k2}, \dots, v_{kn})'$; v_k^* 为 v_k 的伴随向量,且 $v_k^* v_k = \delta_{kk'}$ 。

$$\begin{cases} 1, K = k' \\ 0, K \neq k' \end{cases}$$

v_k 必须满足归一化和零均值条件:

$$\sum_{i=1}^N v_{ki} = 0, \|v_k\|_2 = (\sum_{i=1}^N v_{ki}^2)^{1/2} = 1 \quad (2)$$

定义序参量 ξ_k 为:

$$\xi_k = v_k^* q = v_k q^* \quad (3)$$

把式(3)代入式(1),得到序参量方程为:

$$\dot{\xi}_k = \lambda_k \xi_k - B \sum_{k'=1}^M \xi_{k'}^2 \xi_k - C (\sum_{k'=1}^M \xi_{k'}^2) \xi_k \quad (4)$$

式(4)表明了只有一个全局稳定点,无伪状态、向前竞争、连续的协同演化动力学方程。序参量的引入使原动力学演化方程中的阶次由8次变成了2次,减少了计算量。

1.2 初始序参量特性

当 $\lambda_k = C > 0$, 即注意参数相等时,使用 $D = (B + C) \sum_{k'=1}^M \xi_{k'}^2$, 式(4)简化为:

$$\dot{\xi}_k = \xi_k (\lambda - D + B \xi_k^2) \quad (5)$$

若 $\xi_i < \xi_j$, 由式(5)知,必有 $\dot{\xi}_i < \dot{\xi}_j$, 说明所有的序参量演化轨迹是不会交叉的,初始最大的序参量在协同演化中必然获得胜利。因此系统的终态取决于输入向量的初始序参量值,即在竞争中,具有最大初始序参量的 v_k 获胜,其序参量 ξ_k 趋向于1,而其他序参量趋向于0。

根据协同学的支配原理,系统演化的结构即系统的有序化只取决于非稳定模,称非稳定模为序参量。稳定模依赖于非稳定模,逐渐衰弱,系统状态将由一个最强的非稳定模决定。若把试验模式看成原型模式的线性组合,序参量就代表了输入模式对原型模式分解的系数,输入模式越接近原型模式,这个系数越大,相应的序参量就越大,在竞争中获胜的可能性也就越大。在演化过程中,序参量代表了各个原型模式参与竞争,获胜的序参量代表了被识别的原型模式。

2 图像水印序参量计算

2.1 水印嵌入与提取

图像数字水印算法包含水印嵌入和水印提取两个过程。在不考虑水印的安全性情况下,嵌入过程为:

$$c_w = E(c_0, m) \quad (6)$$

表示载体图像 c_0 和水印 m 通过嵌入函数 E , 在载体图像的空域或变换域中嵌入水印,形成含水印载体图像 c_w 。

水印提取过程为:

$$m_n = D(c'_w, m, c_0) \quad (7)$$

在检测到水印存在的前提下,从含水印载体图像 c'_w 中运用提取函数 D , 提取出水印 m_n 。含水印载体信息 c_w 在传输和使用中会受到可能的信号处理和几何失真等操作的影响,由 c_w 改变为 c'_w 。根据是否使用原始水印 m 或载体图像 c_0 , 确定一定的提取方法 D , 水印的提取是水印算法中最重要的步骤。能否提取出水印,关键在于水印能否承受图像操作的鲁棒性能。

空域图像水印算法的鲁棒性差,水印信息很容易被滤波、加噪、几何变形等操作破坏,主要应用于脆弱性水印中。变换域图像水印算法,大部分采用扩频通信 (spread spectrum communication) 技术,主要思想是在图像的 DCT 变换域里,选择中低频系数叠加水印信息。还可在离散傅里叶变换 (DFT)

或离散小波变换 (DWT) 的频域系数里叠加水印。虽然此类算法的嵌入和提取操作较复杂,隐藏信息量不能很大,但具有承受图像操作能力强、隐蔽性好的特点,很适合于数字图像的版权保护。

本文为了集中研究图像水印的鲁棒性,借鉴文献[3]的嵌入算法,使用一种简化的 DCT 域图像水印嵌入方法,将 ORL 人脸库中的一幅大小为 64×64 的人脸灰度图像 m 嵌入到 256×256 的 Lena 灰度图像 c_0 里。嵌入的具体过程,是先分别对人脸图和 Lena 图进行二维 DCT 变换,对 DCT 系数矩阵 Zig-Zag 扫描排列转换,得到相应的一维向量 x 和 v 。使用运算式 $v'_i = v_i + 0.1x_i$, 把人脸图像的全部 DCT 系数 x_i 嵌入到 Lena 图最重要的相应 DCT 系数 v_i 中,得到改变的一维向量 v' 。 v' 还原成新的 DCT 系数矩阵,再二维 DCT 反变换得到含水印的 Lena 图像 c_w , 结果如图 1 (图中为非原始比例大小)。从水印嵌入过程可得,水印的提取是嵌入的逆过程。

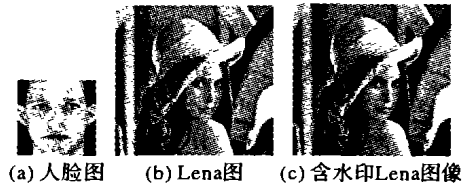


图1 水印嵌入

2.2 序参量计算

具有版权的任何人在水印载体图像中提取和恢复水印,可认为是在已知水印模式集中识别一个特定水印模式的过程,能使用基于协同理论的模式识别的有关概念和方法。协同序参量 ξ_k 的初始值,代表了原型模式和试验模式之间的一种匹配度量。可根据初始序参量的相对大小,识别水印模式,定量评价水印的鲁棒性。

虽然考察的是图像水印的鲁棒性,而不是安全性,但还是希望图像水印算法满足 Kerckhoffs 准则,即要求水印的嵌入和提取算法是公开的。已知水印提取算法时,协同序参量计算步骤为:

1) 确定水印模式集,从 ORL 人脸库再选取 4 幅人脸图,与作为水印的人脸图组成水印模式集,如图 2 所示,水印模式编号为 1 到 5。模式数 $M = 5$ 。



图2 水印模式集

2) 构造模式特征向量,人脸图像灰度矩阵向量化,形成每个模式的特征向量,模式维数 $N = 4096$, 有 $M < N$ 。

3) 依式(2)计算水印模式集的原型模式向量 v_k 及其伴随向量 v_k^* , k 的取值从 1 到 5 (下同)。

4) 从 c_w 提取水印,即为水印 m_0 。与 2) 和 3) 一样,计算 m 的状态向量 q_0 , q_0 也满足归一化和零均值条件:

$$\sum_{i=1}^N q_{0i} = 0, \|q_0\|_2 = (\sum_{i=1}^N q_{0i}^2)^{1/2} = 1 \quad (8)$$

5) 计算未对 c_w 作任何操作的初始序参量 $\xi_k(0) = v_k^* q_0$ 。比较 $\xi_k(0)$ 之间的大小,根据上述理论, $\xi_k(0)$ 中最大的一个就决定了水印是水印模式集中的某一个。

6) 对 c_w 作操作处理得到 c'_w , 提取水印为 m' 。同 4) 和 5), 计算初始序参量 $\xi'_k(0)$ 。

7) 比较 $\xi_k(0)$ 和 $\xi'_k(0)$, 定量评价此水印的鲁棒性。可使用对式(4) 离散化的序参量迭代方程, 计算和绘制各模式序参量的演化曲线, 验证结果。

3 鲁棒性实验与分析

在 MATLAB6.1 中, 分别对水印载体图像 c_w 进行加性噪声、幅度变化、线性滤波、有损压缩和几何失真等不同类型不同强度的操作, 然后从 c'_w 提取水印, 用上文的步骤计算其协同序参量初始值, 获得鲁棒性评价结果。

3.1 未做如何处理操作

直接提取水印, 计算各模式的初始序参量 $\xi'_k(0)$, 得到表 1。

表 1 序参量初始值

序号 1	序号 2	序号 3	序号 4	序号 5
1	2.0893e-016	5.6452e-016	4.2951e-016	-6.5404e-016

水印模式的初始序参量值为 1, 其他模式的值很小。毫无疑问, 嵌入的水印是模式 1 图像。

3.2 加性噪声

加性噪声是图像在传输和使用过程中, 附加上的与图像相互独立的随机信号噪声, 如高斯白噪声等。加噪实验采用高斯噪声和椒盐噪声, 对水印载体图像加均值为 0、方差从 0.0001 到 0.009 的高斯噪声和均值为 0、方差从 0.001 到 0.009 的椒盐噪声。

高斯噪声时, 水印模式的初始序参量值从 0.84748 到 0.15614。椒盐噪声时, 水印模式的初始序参量值从 0.85963 到 0.44408。比其他模式的初始序参量值大一个数量级, 且随着噪声强度的增加, 值是逐步减少的。可得到水印的正确识别结果, 具有对这两种噪声的鲁棒性, 且随噪声强度的增强, 鲁棒性是下降的。

3.3 JPEG 压缩

图像的主要能量集中于低频分量上, 图像压缩算法一般是把当作冗余信息的高频分量清除掉, 用得较多是 JPEG 压缩。压缩实验采用压缩质量从 90% 到 10% 的 JPEG 压缩。水印模式的初始序参量值从 0.95121 到 0.21758, 明显比其他模式的大一个数量级, 且随着压缩质量的下降, 初始序参量的值是逐步减少的。

3.4 滤波

图像水印应具有低通特性, 即低通滤波应该无法删掉图像中的水印。分别进行 3×3 的中值滤波和维纳滤波后, 提取水印, 计算初始序参量的结果如表 2 所示。

表 2 滤波的初始协同序参量

	类型				
	1	2	3	4	5
中值	0.62082	-0.05622	0.058281	0.058162	-0.014289
维纳	0.70868	-0.011683	0.018007	0.054957	0.0016545

水印模式的初始序参量值比其他模式的大, 可获得正确的水印判别结果。

3.5 幅度变化

一些常规的图像量化与增强操作, 均不应对手印的提取和检测有严重影响。实验中, 用灰度从 $[0.1 \ 0.9]$ 到 $[0 \ 1]$ 的对比度增强、从 $[0 \ 1]$ 到 $[0.1 \ 0.9]$ 的对比度减弱和灰度均衡

操作后, 提取水印, 计算初始序参量, 结果如表 3 所示。

表 3 幅度变化的协同序参量初始值

	类型				
	1	2	3	4	5
对比度增强	-0.03506	-0.030147	0.2545	-0.010179	-0.12084
对比度减弱	0.17858	0.06883	-0.22994	0.099013	0.12432
灰度均衡	-0.034934	-0.059561	0.22578	-0.036186	-0.17464

水印模式的初始序参量值不比其他模式的大, 得不到正确的水印判别结果, 在图像幅度变化后, 此水印方案的水印生存可能性很小。

3.6 几何操作

几何失真操作包括图像尺寸大小变化、图像旋转、裁剪、删除或增加图像线条以及反射等等。很多水印算法对这些几何操作都非常脆弱, 容易被去掉。分别进行 $\pm 1^\circ$ 以内的几何旋转操作和 1.01 到 1.1 倍的几何放大操作, 对变大后的水印载体图像剪切为原来大小, 提取水印, 计算初始序参量

在几何旋转度数小于 1° 以内, 水印模式初始序参量比其他模式的大, 且随着旋转角度的加大, 值是逐步减少的。放大后, 水印模式初始序参量比其他模式的大一个数量级以上, 且随着放大倍数的加大, 值也是逐步减少的。可见, 能承受微量的图像旋转、放大和裁剪, 具有一点程度的鲁棒性。

作为本文示例, 图 3(a) 是对含水印 Lena 图像加均值 0、方差 0.009 高斯噪声的处理。从演化图可以看出, 迭代运算不到 100 步, 代表模式 1 的序参量最终演化到 1, 其他模式的趋向 0, 说明使用协同序参量具有非常好的计算性能。

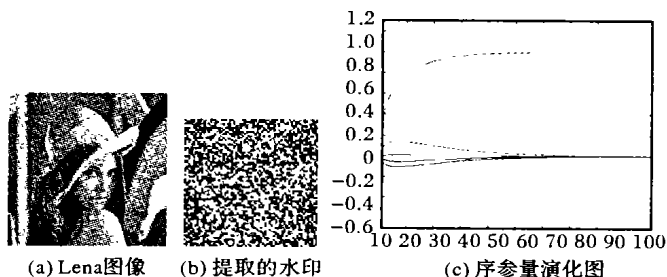


图 3 均值为 0、方差为 0.009 高斯噪声

4 与相关系数的比较

为说明此方法的可行性, 与相关分析中通常所使用的的相关系数数量方法比较。两个图像的相关系数为:

$$\rho(W, W') = \frac{\sum_{i=1}^{N_w} w(i)w'(i)}{\sqrt{\sum_{i=1}^{N_w} (w(i))^2} \sqrt{\sum_{i=1}^{N_w} (w'(i))^2}} \quad (9)$$

其中 $w(i)$ 和 $w'(i)$ 是二维图像灰度矩阵的一维向量化表示, N_w 是向量的长度。 ρ 的大小反映了两个图像的相关性, 值越大说明图像越相似。表 4 是未经处理和经上文操作类型鲁棒性实验处理后提取水印与模式集的部分相关系数计算结果。

从表 4 可知, 直接提取的水印与 5 个模式的相关系数都大于 0.95, 模式 1 图像与其他图像模式有极高的相关性。常规图像操作后提取的水印与各个模式的相关系数大于 0.5, 每类操作的 5 个相关系数的取值都极为接近, 且相关系数相

互之间的大小关系与初始序参量的相同。可见,用初始序参量定量评价图像水印的鲁棒性,与用相关系数的评价是一致的,但更易区分。

表4 相关系数

	1	2	3	4	5
未处理	1	0.9585	0.9548	0.9645	0.9504
高斯噪声 (方差0.001)	0.8846	0.8531	0.8544	0.8641	0.8452
椒盐噪声 (方差0.005)	0.9062	0.8686	0.8677	0.8776	0.8668
JPEG 压缩(50%)	0.9593	0.9158	0.9191	0.9284	0.9110
中值滤波	0.9292	0.8868	0.8953	0.9030	0.8830
维纳滤波	0.9527	0.9114	0.9127	0.9218	0.9034
对比度增强	0.7174	0.7084	0.7353	0.7320	0.7149
对比度减弱	0.9419	0.9365	0.9303	0.9455	0.9546
灰度均衡	0.6357	0.6246	0.6523	0.6495	0.6301
旋转(0.05)	0.7943	0.7688	0.7746	0.7872	0.7782
放大(1.05)	0.9419	0.9271	0.9274	0.9403	0.9419

5 结语

协同序参量是一种宏观参量,用于描述系统的整体行为,

主宰着系统演化过程。系统从无序转变为有序以及从有序转变为更为复杂的有序过程,也就是在一再形成新的自组织过程中,序参量支配其他稳定模而形成了一定的结构或序。系统状态将由一个最强的初始序参量决定,获胜的序参量代表了被识别的原型模式。

协同序参量方法和相关系数法应用于图像水印鲁棒性评价中,所获得的结果是一致的。用初始序参量定量来定量评价图像水印的鲁棒性,理论依据充分,计算简单,识别结果明显。本方法还特别适用于对含水印载体图像声称具有版权的多个嵌入者的场合。在发生版权争议时,仲裁者可用各人的水印组成水印模式集,计算协同序参量的初始值,从而判断图像的归属。

对模式集中模式数量较大的情况,初始序参量的计算和比较还有待进一步研究。

参考文献:

- [1] COX IJ, MILLER ML, BLOOM JA. 数字水印[M]. 北京: 电子工业出版社, 2003.
- [2] HANKEN H. Synergetic computers and cognition - a top-down approach to neural nets[M]. Berlin: Springer-Verlag, 1991.
- [3] COX IJ, KILIAN J, LEIGHTON T, et al. A Secure, Robust Watermark for Multimedia[A]. Proceedings of the First International Workshop on Information Hiding[C], 1996. 185-206.

(上接第382页)

$(ID_S, N_S, m, f^{d_1}(m))$ 发送给银行 B , B 验证收到的签名, 并检查 m 在以前是否被花费过。如果签名合法并且 m 没被花费过, 那么银行 B 就在 S 的账号 N_S 上存入 A 发给 S 的货币。售票实体收到货币之后, 它对 x' 签名得 $y' = \text{Sig}_T(x') = (x')^{d_1} \bmod n_1$, 然后售票实体把签名 y' 发送给客户, 客户把盲因子去掉, 计算: $y = y' / k \bmod n_1 = (f_1(x)k^{e_1})^{d_1} / k \bmod n_1 = f_1^{d_1}(x) \bmod n_1$, y 是 x 的合法签名, 也就是客户从售票实体那里得到的票。利用这张票, 客户再向时间戳服务请求给文档 Hash 值加盖时间戳。

2.2 加盖时间戳过程

时间戳服务实体选择两个大素数 p_2 和 q_2 , 以及一个安全 Hash 函数 f_2 , 并随机选择 e_2 , 使得 $\gcd(e_2, \varphi(n_2)) = 1$, 其中 $n_2 = p_2 q_2$, 由 $e_2 d_2 = 1 \bmod \varphi(n_2)$ 知 $d_2 = e_2^{-1} \bmod \varphi(n_2)$ 。时间戳服务公布 n_2, e_2, f_2 , 保密 p_2, q_2 和 d_2 。

客户如果要对一个文档 m_2 加盖时间戳, 客户首先计算 $z_2 = h_2(m_2)$, 其中 h_2 是安全的 Hash 函数。客户发送 (y, x, z_2) 给时间戳服务。

时间戳服务收到 (y, x, z_2) 之后:

1) 首先验证票 y 是否有效:

时间戳服务得到售票实体的公钥 (e_1, n_1) ; 计算 $y^{e_1} \bmod \varphi(n_1)$; 时间戳服务计算 $f_1(x)$; 如果 $y^{e_1} \bmod \varphi(n_1) = f_1(x)$, 则票有效, 可以给它加盖时间戳; 否则, 票无效。

2) 其次在客户的票被验证有效之后, 给 z_2 加盖时间戳:

时间戳服务得到当前的日期和时间 t ; 时间戳服务计算: $\hat{z}_2 = f_2(z_2 \| t)$; 时间戳服务对 \hat{z}_2 签名, 计算: $z' = (\hat{z}_2)^{d_2} \bmod \varphi(n_2)$; 时间戳服务公布 (z', \hat{z}_2, t) 。

2.3 客户验证过程

客户得到时间戳服务公布的 (z', z_2, t) 之后, 可以验证时间戳的有效性, 验证过程如下:

1) 客户得到时间戳服务的公钥 (e_2, n_2) ;

2) 客户计算 $(z')^{d_2} \bmod \varphi(n_2)$;

3) 客户计算 $f_2(z_2 \| t)$;

4) 比较, 如果 $(z')^{d_2} \bmod \varphi(n_2) = f_2(z_2 \| t)$, 则时间戳有效, 客户把它保存起来; 否则, 时间戳无效, 客户应请求时间戳服务重新加盖一次时间戳。

3 结语

随着我国数字签名法的即将出台, 安全数字时间戳也将具备法律效力, 其重要性不言而喻。本文基于 RSA 数字签名, 提出了一种新的安全数字时间戳方案, 新方案通过引入一个售票实体成功地解决了服务付费问题。并且基于 RSA 数字签名, 构造了一个完整的安全数字时间戳系统。

参考文献:

- [1] LIPMAA H. Secure and efficient time-stamping systems[J]. Ph. d, University of Tartu - Estonia, July 1999.
- [2] MASSIAS H, AVILA XS, QUISQUATER J-J. Timestamps: Main issues on their use and implementation[A]. IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises[C], 1999.
- [3] Protocols and data formats for time-stamping service[J]. 17th September 2002.
- [4] HABER S, STORNETTA WS. How to Time-Stamp a Digital Document[J]. in Journal of Cryptology, 1991, 3(2): 99-111.
- [5] BULDAS A, LAUD P, LIPMAA H, et al. Time-stamping with binary linking schemes[Z]. Advances in Cryptology-CRYPTO'98, LNCS1462, 1998.
- [6] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 2001.
- [7] STADLER M, PIVETEAU JM, CAMENISCH J. Fair Blind Signature[J]. Advance in Cryptology-Eurocrypt'95, Springer-Verlag, 209-219.