基于WAP的移动电子商务支付系统安全性改进①

肖 荣 张云华 (浙江理工大学 信息电子学院 浙江 杭州 310018)

章依凌 (浙江理工大学 服装学院 浙江 杭州 310018)

摘 要: 为了解决移动支付的安全问题，研究了基于 WAP 的移动电子商务支付系统的安全性，创新地引入了信息隐藏和数字水印的概念，提出了一种抗 GSM 语音压缩编码的 ERA 算法，将音频数字水印加入到系统，大大加强基于 WAP 的移动电子商务支付系统的安全性。

关键词: 无线通讯协议；信息隐藏；频数字水印

Improvement of Secure Mobile E-Commerce Payment System Based on WAP

XIAO Rong[1], ZHANG Yun-Hua[1], ZHANG Yi-Ling[2]

(1.Department of Information & Electronics, Zhejiang Sci-Tech University, Hangzhou 310018, China;
2.Department of Fashion Design & Engineering, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: To gurantee the safety of mobile payment, this paper conducts a study on the security of the mobile e-commerce payment system based on WAP. It introduces the concept of information hiding and digital watermarking, and puts forward an anti-GSM voice compression coding algorithm based on ERA(Energy Ratio Adjustment). Moreover, the audio digital watermark is added to the system which has greatly strengthened the security of the WAP- based mobile e-commerce payment system.

Keywords: WAP; information hiding; audio digital watermark

1 引言

近年来，全球移动支付市场呈现高速增长的发展态势。全球移动支付收入自 2004 年起实现成倍增长，从 2002 年的 55 亿美元，增长到 2007 年的近 800 亿美元。从交易规模来看，根据研究咨询公司 BWCS 的预测，预计到 2010 年，全球仅移动现场支付的市场规模将达到 3800 亿美元[1]。移动支付作为第三方电子支付的一种，随着市场需求和用户数量的迅速上升，其市场空间逐步放大。

随着电子商务架构逐步服务于多种移动终端，WAP 将在移动新经济中占有重要的一席之地。目前，WAP 已取得了包括手持设备制造商、无线架构供应商及无线应用软件商在内的众多业界领先供应商的鼎力支持。随着移动设备的日趋广泛和普及，将有望使 WAP 成为主导未来移动电子商务架构的主流技术。

2 基于WAP的支付系统安全性分析

基于移动网络的电子商务因为其便捷、灵活的特点而越来越受到人们的欢迎，然而移动支付尚未得到广泛普及，其中的一个主要因素在于移动支付的安全问题。基于 WAP 的移动支付系统安全性是建立在 WAP 的基础上的。但目前这种系统还存在以下缺点：

(1) 移动终端只能通过 B/S 方式访问因特网。WAP 是一种分层协议：底层是无线 WDP、WTP 等传输层协议，基于此上应用层中的 WAP 微浏览器只能访问 WML 脚本，而不是主流的 HTML，也不能显示复杂格式的图形。

(2) WAP1.X 解决方案需要移动终端手机通过

① 收稿时间:2009-06-16

WAP 网关才能访问因特网，由于 WAP 网关的存在不可避免地带来新的安全隐患，例如中间人攻击等。直到 WAP2.0 采用 TLS 来保证端到端的安全性。

(3)WAP 解决方案不能访问终端设备本地存储区，需要运行于在无线环境中。大量数据的交换增加了服务器负荷，并且增加了数据被窃听的可能性。

目前IVR、SMS和WAP都属于电路承载型的业务，但它们所使用的电路信道不尽相同：通话状态下，IVR 和 SMS 使用相同的信令信道即 SDCHH，数据传输速率大约为 600bps，WAP 数据传输速率大约为 1Kbps，比 SMS 传输速率高。目前，用户只能在非通话状态下使用 WAP，数据通过语音信道 TCH 进行交换，其传输速率大约为 9.6 Kbps；随着 GPRS、3G 等移动通信技术的发展和成熟，WAP 将演进为分组交换型业务，其数据传输速率也将达到 115.2 Kbps(GPRS 的一般速率)，甚至达到 2Mbps。可以看出基于 WAP 的移动支付将有很大的发展空间。

3　抗GSM语音压缩编码的水印嵌入算法

3.1 算法介绍

信息隐藏是把有意义的信息隐藏在另一个称为载体的信息中得到隐秘载体，使窃听者察觉不到隐秘载体中隐藏了其他信息，以达到信息安全传输目的的方法。数字水印技术是信息隐藏的一种，从狭义上来讲是将一些特定信息，按照某种方式植入被保护信息中。当被保护信息在网络传播或其它状态下被非法复制从而产生版权纠纷或信息被非法篡改时，通过相应的算法提取出该数字水印，从而验证版权的归属或原始信息(被保护信息)的完整性，确保著作权人的合法利益以及鉴别信息的真伪。数字水印是嵌入在数字产品中的数字信号，水印的存在要以不破坏原数据的欣赏价值、使用价值为原则。

文献[2]提出了一种伪装数字化语音保密通信系统。该系统将需要传输的密文语音信息利用 MELP 算法编码后，使用 ABS 算法隐藏到一段 GSM 编码的明文语音中传输。这样窃听者听到的是一段正常的明文语音信息，不容易引起怀疑，使得密文信息能够安全传输，但是这种方法要求对现有手机的 GSM 语音编码电路进行改造，在其中嵌入 ABS 算法，实现难度较大。

为了获得一种能够和现有大多数 GSM 手机兼容的语音隐藏移动通信系统，要求设计一种算法能够在手机 GSM 语音编码芯片之前完成信息隐藏，并且能够抵抗 GSM 编码解码，最终在接收端正常解出隐藏的密文信息。这种算法的关键在于能够抵抗 GSM 语音编解码，即 GSM 编解码不会影响隐藏信息的嵌入。经过研究发现一段语音经过 GSM 编解码以后，输出语音和原始语音的相邻段能量比基本保持一致。基于此特性，本文提出了一种新的能够抵抗 GSM 语音编码的信息隐藏算法。其原理为将明文语音分段，根据密文信息调整相邻段之间的能量大小，在接收端根据相邻段之间的能量大小进行解码。大量仿真试验结果表明该算法能够抵抗 GSM 编码解码，其明文语音质量下降不多。每秒明文能够嵌入 50bit 的密文信息。实验证明这是一种简单有效的 GSM 移动通信系统语音隐藏算法。

3.2 算法实现

3.3.1 基于功率调整(ERA)的抗 GSM 编码的语音水印嵌入方法

ERA 语音水印嵌入算法的流程图如图 1 所示：

具体实现流程如下：

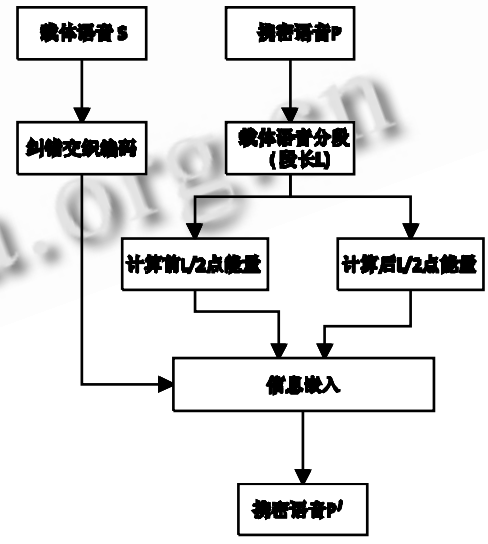

图 1　ERA 语音水印嵌入算法流程框图

(1) 将需要隐藏的水印信息 S 使用 Gray 码进行纠错交织编码，形成 q bit 的隐藏信息 X：

$$X=\{x(i),0<i<q\} \qquad x(i)\in\{0,1\}$$

(2) 将明文语音 P 进行分段，设 $P=\{p(j),0<j<M$ 为 M 个样点的公开语音，分段后表示为：

$$p(k)=p(k\times L+j)\quad 0<k<K \text{ 且 } 0<j<L$$

$p(k)$ 表示第 k 段语音，K 表示明文语音的总段数，L 表示每段样点数。若要保证隐藏信息 X 能够完整嵌入，必须满足：$q\le L$或者$q\times L\le M$ 。

将 P 分段分别计算前 L/2 个点的能量 E_1和后 L/2 个点的能量 E_2：

$$E_1=\sum_{j=0}^{L/2-1}(p(k\times L+j))^2 \qquad E_2=\sum_{j=L/2}^{L}(p(k\times L+j))^2$$

在对应段嵌入信息。由于透明性和鲁棒性是一对矛盾，嵌入深度 β 增加，鲁棒性随之提高，但势必导致携密语音 P′ 质量的下降，因此 β 应依据具体应用条件适当选取。

将 $x(i)$ 嵌入到 P 中的具体过程如下：

首先计算前 L/2 段的放大增益：

$$\beta_1=\begin{cases}\sqrt{\beta\times E_2/E_1} & x(i)=1 \text{且} E_2/E_1<\beta\\ 1 & \text{其他}\end{cases}$$

其次计算后 L/2 段的放大增益：

$$\beta_2=\begin{cases}\sqrt{\beta\times E_1/E_2} & x(i)=0 \text{且} E_2/E_1<\beta\\ 1 & \text{其他}\end{cases}$$

最后根据 β_1 、β_2 的值将嵌入到明文语音 P 中。从而获得携密的明文语音 P′ 进行存储或传输。

3.3.2 水印信息提取算法

水印信息提取算法的流程图如图 2 所示：

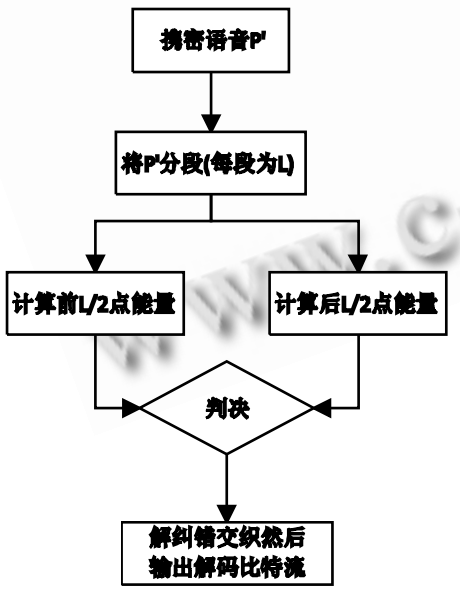

图 2　水印提取算法流程图

在水印信息提取时，首先将接收到的携密的明文语音 P′ 进行分段处理，每段段长为 L 个采样点。分段后表示为：

$$p'(k)=p'(k\times L+j)\qquad 0<k<K\text{且}0<j<L$$

然后计算前 L/2 点能量 E_1'和后 L/2 点能量 E_2'：

$$E_1'=\sum_{j=0}^{L/2-1}(p'(k\times L+j))^2 \qquad E_2'=\sum_{j=L/2}^{L}(p'(k\times L+j))^2$$

最后进行判决获得通过信道的密文信息 X'。

判决规则如下：

$$X'(i)=\begin{cases}1 & E_1'>E_2'\\ 0 & E_2'>E_1'\end{cases}$$

将经过解交织解纠错编码即可得到恢复出的密文信息。

3.3 实验过程及性能分析

在实验中为了验证绝大多数情况，我们选用了两段长短不同的，男女都有的录音讲话，Hello.wav，Talk.wav，并在网上下载了一段讲话录音 Speech.wav 。它们的位速分别为 280kbps，150kbps，80kbps，采样频率为 22KHz。图 3，4，5 分别为三段录音未嵌入水印前的波形图。

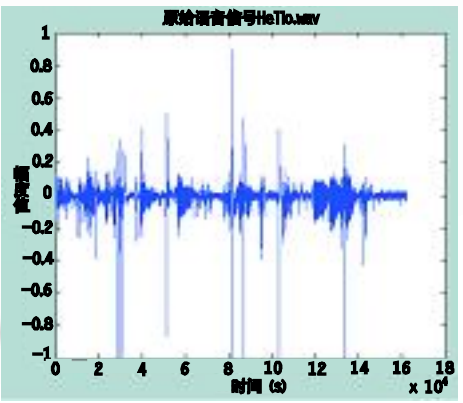

图 3　原始音频信号 Hello.wav 波形图

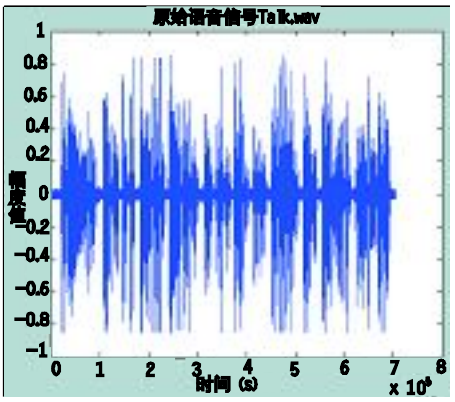

图 4　原始音频信号 Talk.wav 波形图

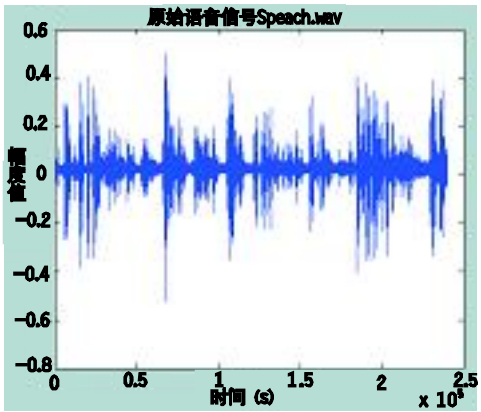

图 5　原始音频信号 Speech.wav 波形图

为了测试该算法的性能，进行了各类仿真实验。实验中的数据均采用 8KHz 采样,16bits 量化的语音，语音 S 共 28000 个采样点。语音段长 L 为 160 个采样点，嵌入深度 =1.5。分别在无攻击和多种攻击情况下分析本文算法的性能。本文衡量音质的主要性能指标有归一化相关系数、分段平均信噪比[3]。

3.3.1 携密语音 P′ 的质量

携密语音 P′ 的质量的好坏反映了算法的透明性指标，是衡量算法好坏的重要标志。

表 1 给出了本算法在无攻击情况下的分段平均信噪比 SNR(dB)和原始明文和携密明文归一化相关系数指标。

表 1　无攻击情况下携密语音 P′ 的音质

算法	SNR(dB)	$\rho(p,p')$
GSM 能量隐藏算法	33.8	0.980

从主观听觉测试结果表明，本文所提算法获得的携密语音仅仅比原始明文略多一点噪声，并不影响整体听觉效果。

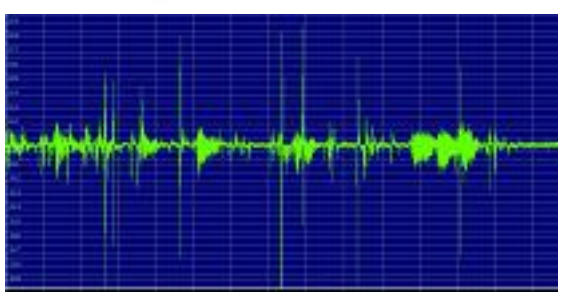

图 6　携密语音 HelloGsm.wav 的波形图

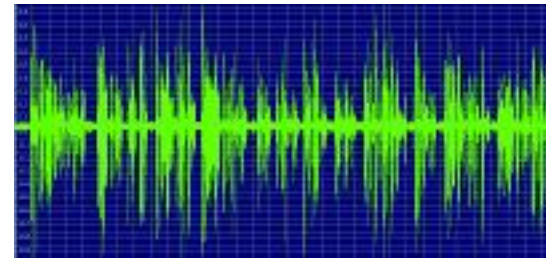

图 7　携密语音 TalkGsm.wav 的波形图

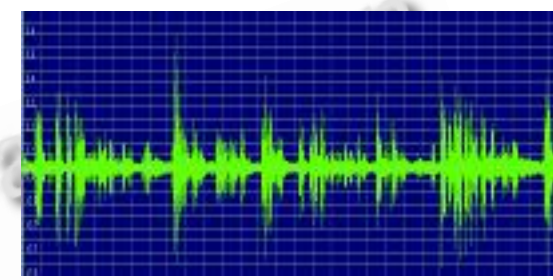

图 8　携密语音 SpeechGsm.wav 的波形图

图 6，7，8 分别为携密语音 HelloGsm.wav，TalkGsm.wav，SpeechGsm.wav 经过 GSM 编码之后的波形图。

3.3.2 抗语音压缩测试

抗压缩能力是衡量算法鲁棒性的重要指标，也是通信网络环境对实用信息隐藏技术的要求。为了测试本文所提算法抵抗语音压缩的性能,我们将三段中间语音 P′ 分别使用 GSM 语音编码、G.721 32kb/s ADPCM 以及 G.723 24/40kbs 的 ADPCM 编码进行压缩后再进行信息提取。表 2 显示了经过不同语音编码算法处理后信息提取的误码率以及经过纠错以后的误码率。

表 2　本文算法抗压缩性能测试结果

压缩算法	直接提取信息的误码率%	经过纠错后提取信息误码率%
GSM 语音编码	4.02	0
24kb/s ADPCM	0.3	0
32kb/s ADPCM	0	0
40kb/s ADPCM	0	0

3.3.3 抗低通滤波性能

将携密语音 P′ 经过截至频率分别为 500～3500Hz 的低通滤波器,滤波后提取隐藏信息。图 9(a)给出了低通滤波后的性能曲线。图 9(b)表明即使 P′ 在 2KHz 低通滤波的攻击下，经过纠错编码以后仍能

够完全解出隐藏信息。

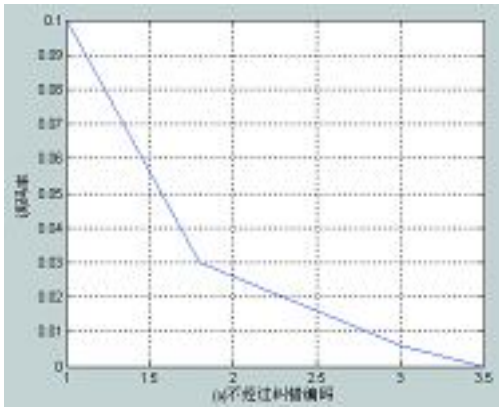

图 9(a) 算法抵抗低通滤波的性能图 1

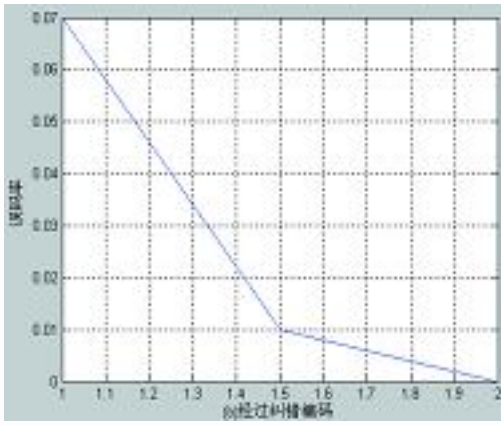

图 9(b) 算法抵抗低通滤波的性能图 2

3.3.4 抗中值滤波性能

中值滤波是语音处理中常用的操作。为了测试本文所提算法抵抗中值滤波的性能，我们将携密语音 P′ 经过窗口长度分别为 3，5，7，9 的中值滤波后，再提取信息。我们用 A 表示未经过 Gray 码纠错实现了信息的成功提取，A+表示经过 Gray 码纠错实现了信息的成功提取，B 表示未经过 Gray 码纠错未能实现信息的成功提取。

表 3 抗中值滤波性能测试统计表

攻击方法 / 语音	中值滤波 3	中值滤波 5	中值滤波 7	中值滤波 9
HelloGsm	A A+	A A+	A A+	A A+
TalkGsm	A A+	A A+	A A+	A B
SpeechGsm	A A+	A A+	A A+	A A+

如上表 3 所示，统计表明直接提取信息后的误码率为 0.5%，而经过 Gray 码纠错后，隐藏信息能够完全恢复。

4 结语

本文研究了基于 WAP 的移动电子商务支付系统的安全性问题，创新地引入信息隐藏和数字水印的概念，提出了一种抗 GSM 语音压缩编码的 ERA 算法，将音频数字水印加入系统，通过实验验证，发现这种算法具有良好的鲁棒性和强的抗低通滤波攻击的能力和抗中值滤波性能，并满足了 GSM 通信中的要求，因而可以大大加强移动电子商务支付系统的安全性。

参考文献

1 唐奕.我国移动支付市场发展[2009-2-10]. http://www.chinaunionpay.com.

2 杨伟,王飞等.伪装式数字化语音保密通信系统.通信学报, 2004,25(2):75－84.

3 陈亮,张雄伟.基于语音参数模型的语音隐藏算法.计算学报, 2003,26(8):974－984.