

به نام خدا

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

صادق سلیمانی^۱، پرینسا کاغذگران^۲

اعضو هیئت علمی دانشگاه کردستان
S.Sulaimany@Uok.ac.ir

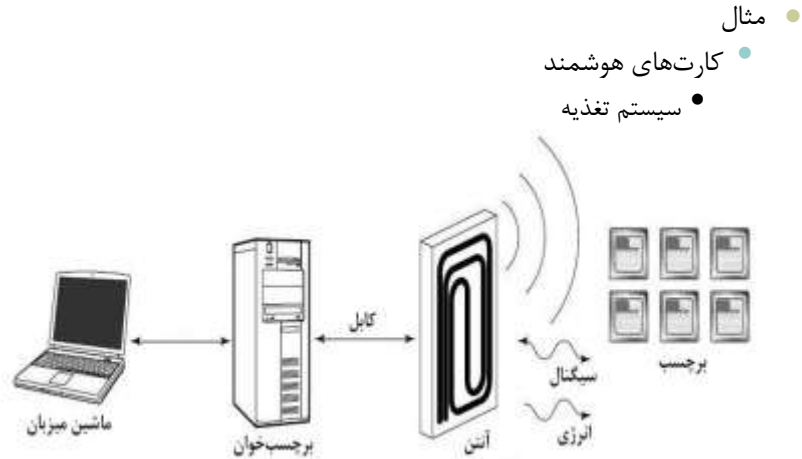
^۲دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر
Parisa.kaghazgaran@gmail.com

فهرست مطالب

- مروری بر RFID
 - ساختار فیزیکی
 - ساختار منطقی
 - مهمترین چالش‌های امنیتی و محرمانگی
- Tamper Protection
 - Watermarking
 - بررسی روش‌های ارائه شده
 - پیشنهاد روش جدید
 - مقایسه روش‌ها

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

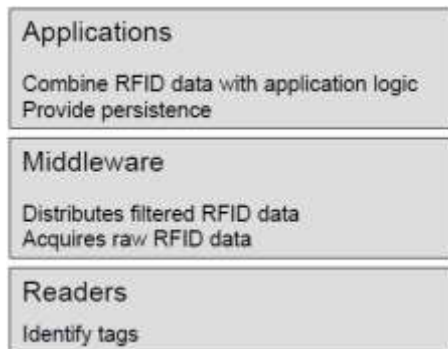
مروری بر RFID



تشخیص دستکاری در داده‌های برجسب RFID با استفاده از نشانه گذاری شکننده 3 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

ساختار منطقی سیستم RFID



تشخیص دستکاری در داده‌های برجسب RFID با استفاده از نشانه گذاری شکننده 4 از 24

عناوین ارائه: مقدمات- Watermarking - رویکردهای تشخیص دستکاری- نتیجه گیری

مروری بر RFID



- رایج ترین استفاده ها
- جایگزینی بارکد
- شناسه ی الکترونیکی کالا
- کاربرد وسیع
- بهای نازل
- تعداد بسیار زیاد

Electronic Product Code •
EPC •

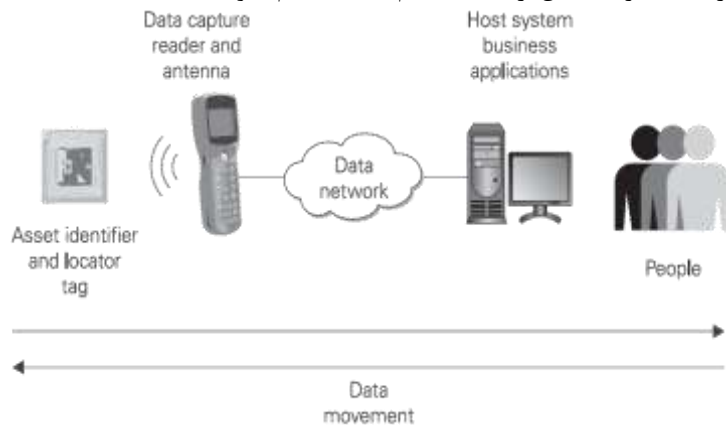
تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده

5 از 24

عناوین ارائه: مقدمات- Watermarking - رویکردهای تشخیص دستکاری- نتیجه گیری

مروری بر RFID

- درک عملکرد با مثال از یک سیستم یک سیستم نمونه



تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده

6 از 24

عناوین ارائه: چالش‌ها - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

از اصلی‌ترین چالش‌ها

• امنیت و صحت

• مثال

- تشخیص کالا (مثلا دارو یا کتاب) مورد استفاده‌ی یک فرد
- تغییر بها یا نوع یک قلم جنس
- تخمین میزان فروش یک شرکت
- ...

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

7 از 24

عناوین ارائه: راه کارها - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

راهکارها

• غلبه بر چالش‌های امنیتی برچسب‌های EPC

• راه حل ۱:

- کشتن برچسب
- همیشه کارساز نیست
- گاهی می‌خواهیم برچسب را در چرخه‌ی عمر آن حفظ کنیم
- مثلا تولید - فروش - گارانتی

• راه حل ۲:

- رمزنگاری
- برچسب‌های ارزان و محدود EPC امکان پیاده‌سازی مدارات رمزنگاری ندارند
- کل Gate‌های یک برچسب EPC، ۲۰۰۰ عدد
- حداقل Gate‌های پیاده‌سازی AES، ۲۵۰۰۰ عدد

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

8 از 24

عناوین ارائه: راه کارها- Watermarking – رویکردهای تشخیص دستکاری- نتیجه گیری

یافتن راهکار امنیتی برچسب

- برچسبها محدودیت‌های زیر را دارند
 - انرژی
 - باتری ندارند
 - مدارات
 - تعداد خیلی کم
 - حافظه
 - ۹۶ بیت

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

9 از 24

عناوین ارائه: راه کارها- Watermarking – رویکردهای تشخیص دستکاری- نتیجه گیری

ساختار برچسب‌های EPC

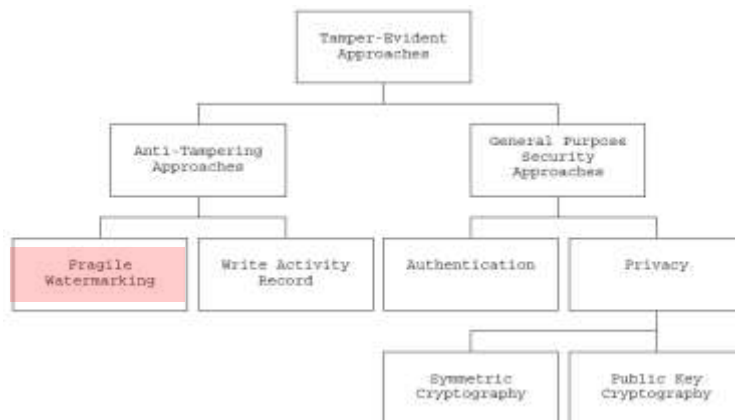


تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

10 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

رویکردهای پیشنهاد شده



تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

11 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

نشانه گذاری (Watermarking)

- افزودن سیگنال یا علامتی به داده‌ی اصلی
- قابلیت برگرداندن (بازیابی) سیگنال در صورت عدم دستکاری داده
- 1. Robust Watermarking
 - حفاظت از Copyright
 - جلوگیری از کپی
- 2. Fragile Watermarking
 - تشخیص تغییر
 - نواختن هشدار
- 3. Semi-Fragile Watermarking
 - هشدار برای برخی تغییرات، نه همه‌ی تغییرات

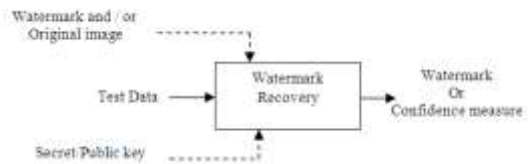
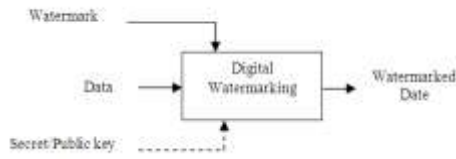
تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

12 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

روند Watermarking

1. طراحی سیگنال نشانه
2. تعبیه‌ی سیگنال نشانه در داده
3. استخراج سیگنال نشانه



تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

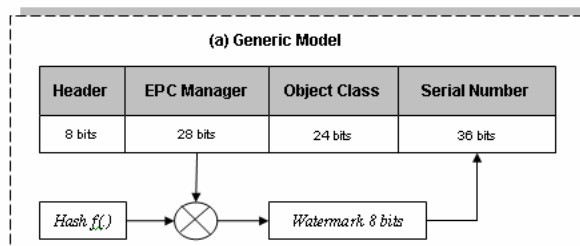
13 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

بررسی روش‌های پیشین

• روش ۱

• Vidyasagar Potdar, Elizabeth Chang از دانشگاه Curtin استرالیا



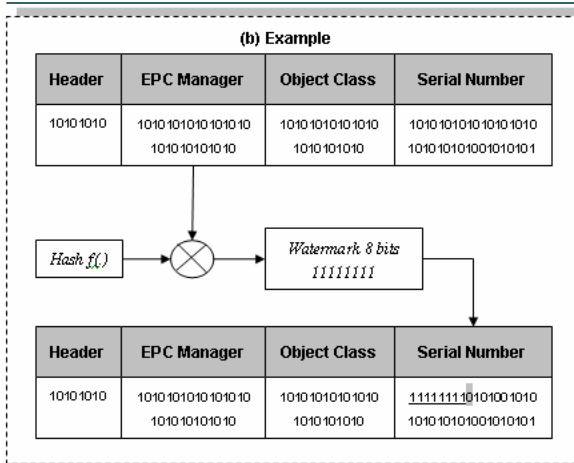
تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

14 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

بررسی روش های پیشین

• مثال از روش ۱



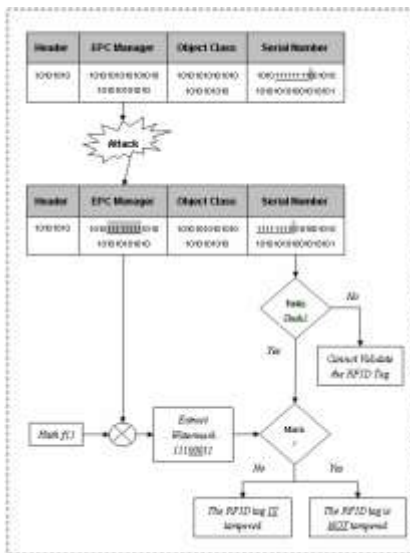
تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده

15 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

بررسی روش های پیشین

• مثال از روش ۱



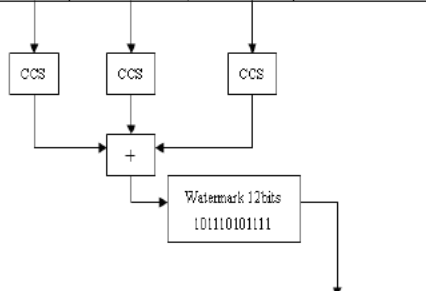
تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده

16 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

بررسی روش های پیشین

Header	EPC Manager	Object Class	Serial Number
10101010	10101010101010	101010101010	10101010101010
	10101010101010	101010101010	10101010101010



Header	EPC Manager	Object Class	Serial Number
10101010	10101010101010	101010101010	111010110101010
	10101010101010	101010101010	1010101010111010

CCS represents coupled chaotic systems.

روش ۲

• استفاده از نظریه آشوب Chaos

• دانشگاه Southwest Jiaotong

چین

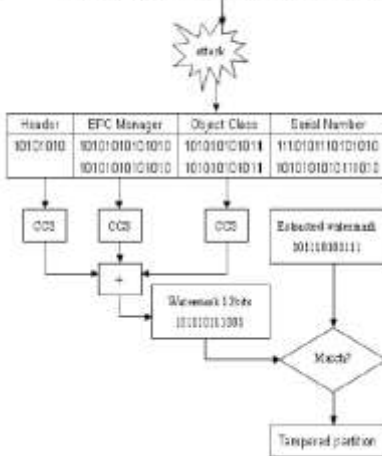
تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده

17 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

مثال از روش ۲

Header	EPC Manager	Object Class	Serial Number
10101010	10101010101010	101010101010	111010110101010
	10101010101010	101010101010	101010101011010

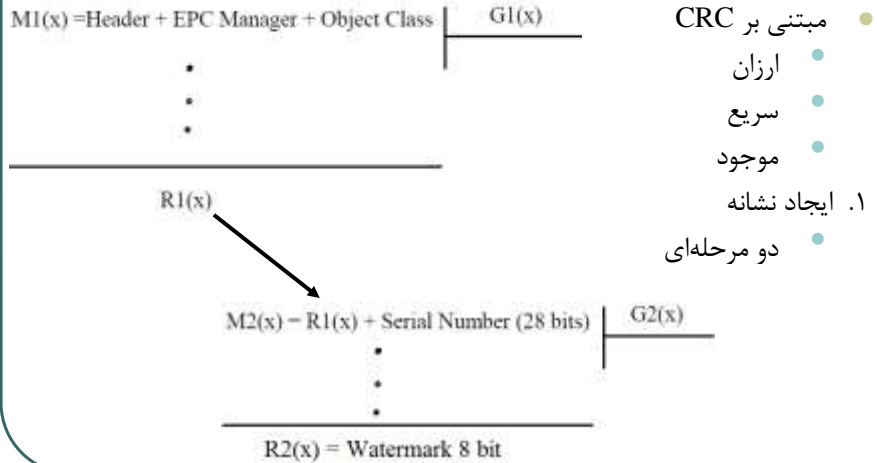


تشخیص دستکاری در داده های برچسب RFID با استفاده از نشانه گذاری شکننده

18 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

روش پیشنهادی



تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

19 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه‌گیری

تشریح روش پیشنهادی

۲. درج نشانه

- درج ۸ بیت در مکان‌های تصادفی در Serial Number
- استفاده از تابع تولید شبه تصادفی برگشت پذیر

$$X_{i+1} = X_i^2 \text{ mod } N$$

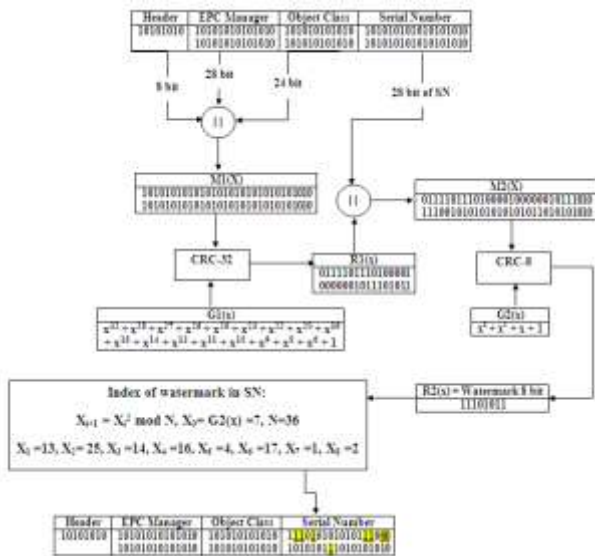
- ۸ عدد تصادفی بین ۰ تا ۳۶
- $x0$ همان $G2(x)$ و $N=36$
- در صورت رویداد عدد تصادفی
- یک واحد افزوده و مجدداً به پیمان‌های ۳۶ برده می‌شود

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

20 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

روش پیشنهادی

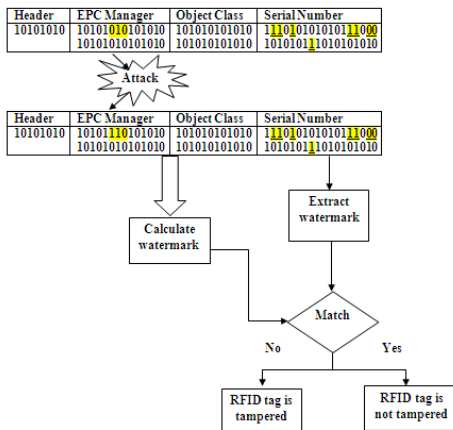


تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

21 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

مثال از روش پیشنهادی



تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

22 از 24

عناوین ارائه: مقدمات - Watermarking - رویکردهای تشخیص دستکاری - نتیجه گیری

مقایسه

سخت افزار	تعداد بیت‌های تحت نظارت	قابلیت تشخیص مکان رویداد دستکاری	مرواحت بیت‌های نشانه	تعداد بیت‌های اختصاصی به نشانه	سرچ
لازم نیست	۲۸	دارد	مشخص	۶	روشن ۱ - رویکرد ۱
لازم نیست	۵۴	دارد	مشخص	۱۸	روشن ۱ - رویکرد ۲
لازم نیست	۶۰	دارد	نامشخص	۱۲	روشن ۲
اختیاری	۸۸	ندارد	نامشخص	۸	روشن ۳

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

23 از 24



با تشکر از حضور و توجه شما

تشخیص دستکاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده

24 از 24