RESEARCH ARTICLE OPEN ACCESS

Tamper Detection Technique in RFID System

*1K.T. Patil, *2Sanket Sonawane, *Saili Shinde, #Dr. S.K. Narayankhedkar
*Smt. Indira Gandhi College of Engineering, Navi Mumbai, India
#MGM College of Engineering and Technology, Navi Mumbai, India
*1ktpatil@rediffmail.com, *2sanketssonawane10@gmail.com

Abstract
Security is one of the major concerns with RFID (Radio Frequency Identification). Due to the advantages offered by RFID in the field of contactless auto identification, it is being used in the widespread range of applications. Data tampering is one of the major issue being encountered. Tag data tampering is one in which by changing the tag contents attackers can mislead the organisations adopting RFID system in their workspace. In order to detect whether the tags are tampered or not, watermarking is embedded in the serial number of the tags. In this paper we have collectively discussed about the existing tamper detection method and provided how 12bits watermarking has an upper hand over the 8 bit watermarking.
Keywords – EPC; OC; data tampering; RFID; fragile watermarking.

I. INTRODUCTION

RADIO frequency identification (RFID) is a technology, in which a tiny Tag contains information related to the object to which it is attached. An RFID system which is shown in Figure 1 typically includes an RFID readerand some RFID tags. RFID system is made up of a reader,which generates an electromagnetic field, and some passive tagswithout an own voltagesupply. They can be read only if they are in the reading range of a reader which suppliesthe power required through a coupling unit. The RFID tags hold a memory thatstores an unambiguous identification code (ID) and potentially a rewritable user memory.RFID technology is mainly used in order to identify objects by matching themwith tags. The Automatic Identification and Data Capture (AIDC) based on RFIDprovides many benefits, such as time saving and great accuracy, at a reduced cost . However, RFID tags are also used for other kinds of operations, such as localization,data storing, and personal identification[1].

Data tampering in RFID tag is one of the threat in which tag data representing identification or location information or specification of object to which it is tagged, its type, price, date of manufacturing-expiry etc, depending on application, is modified by attacker. Such unauthorised alteration of tag data results in great loss. Data tampering can be performed on RFID tags with a rewritable memory, bymeans of a RF communication. According to the pervasive deployment of tags, anattack can be performed moving the adversary RFID reader for few seconds inside thereading range of the tag, or viceversa waiting until the tag is moved in the reading rangeof the hidden adversary RFID reader[2].

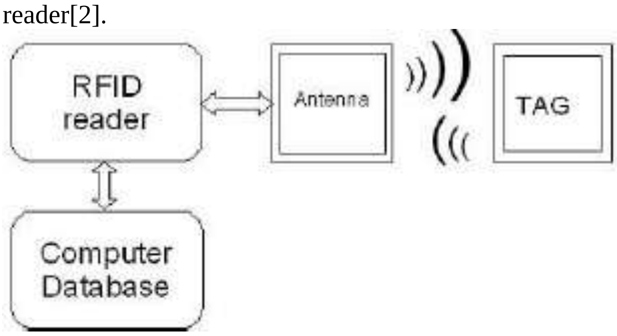


Fig.1 RFID System

For tags with a read-only memory, tamperingattacks cannot be performed by means of a RF communication, so the physical accessto the tag is required in order to perform the more costly hardware tampering. In this paper we have discussed about basic architecture of RFID system, data tampering, existing tamper detection methods and proposed a tamper detection method.

A. EPC structure:

The standardisation bodies such as the EPC global (Electronic Product Code)

- *Header* : determines which EAN.UCC key is used and
- how many bits are allocated to the remaining sections
- *EM(EPC MANAGER)* : identifies the product manufacturer
- *OC(OBJECT CLASS)*: which is a unique identifier for the product manufactured by the manufacturer
- *SN(SERIAL NUMBER)* : which is assigned to

each item belonging to a class of product.

II. TAMPERING ISSUES IN RFID TAG

Several fields in information Technology are subject to the tampering problem, so many effective defenses havebeen proposed. There are two kinds of protections against tampering.Tamper-evidence- The feature of a process, device, or software, to detect the existence of tampering.Tamper-resistance[3]; the ability to resist to tampering.The effects of tampering can be divided in two main groups:damage when tampering makes something unusable;alteration when the target seems correct, but according to the malicious alteration,it is faulty and it will generate possible mistakes.Although tamper-resistance solutions aim at preventing all tampering effects, tamper-evidence aims at preventing only mistakes due to an alteration, reduced to a damage. Inthe following the main tampering effects and tamper-protection schemes from severalfields are introduced, describing their relation with RFID[4].One field in information technology, where the tampering problem has beenProduct Code) and the GS1 (Global Standardization) are working together to propose and manage global standard for RFID tags. EPC Class 1 Generation 2, also known as Gen 2 or EPC-C1G2 is latest standard for 96 - bit EPC tag An (EPC) structure is shown Table. An electronic product code is a universal identifier that gives a unique identity to a specific physical object [3]. This identity is designed to be unique among all physical objects and all categories of physical objects in the world for all time.

Header	**EPC Manager**	**Object class**	**Serial number**
8-bit	28-bit	24-bit	36-bit

Fig: EPC-96 Tag Structure

Widely studied, is the software protection. A tamper attack couldaltera program in someways. An adopted solution is adding tamper-evident features, by inserting into theprogram tamper-proofing code, which can detect if the program was tampered with,stopping the program when tampering effects[6] are detected. This kind of attack couldbe very dangerous for pervasive devices, since they are often deployed into hostile areas.However, low cost RFID tags are very simple devices and most of them do not presmicroprocessor, so software tampering does not represent a relevant threat.A considerable tampering subject is thehardware tampering Tampering actionsmay aim atdamagingthe device or atalteringthe system accessing to the code inorder to

A. Literature survey

reprogram it with a malicious one able to execute insider attacks. The tamper-resistant hardware may avoid unauthorized access to the running code and it may resistto malicious actions such as physical penetration, and temperature manipulation. Various applications employ tamper-resistant hardware, among which several approachesfor authentication and integrity checking in mobile systems. However, the use oftamper-resistant hardware requires high costs, which are often too expensive for pervasiveenvironments. In wireless sensor networks a tampered node with a maliciousrunning program is a critical threat. Hardware tampering attacks to RFID tags havenot been reported[5], and it is not yet directly handled by RFID security approaches forlow cost RFID tags. The main motivation is that tags are often vulnerable to simplerand faster RF attacks, which can be applied also withoutphysical access.Thus tampering in RFID tag refers to altering data stored on RFID tag by attacker for the purpose of its own benefit and / or to disrupt the business of the organizations.

It is necessary to trace out any such data alteration by attackers to avail advantages offered by RFID technology safely and reliably. This is what called as Tamper Detection in RFID system.

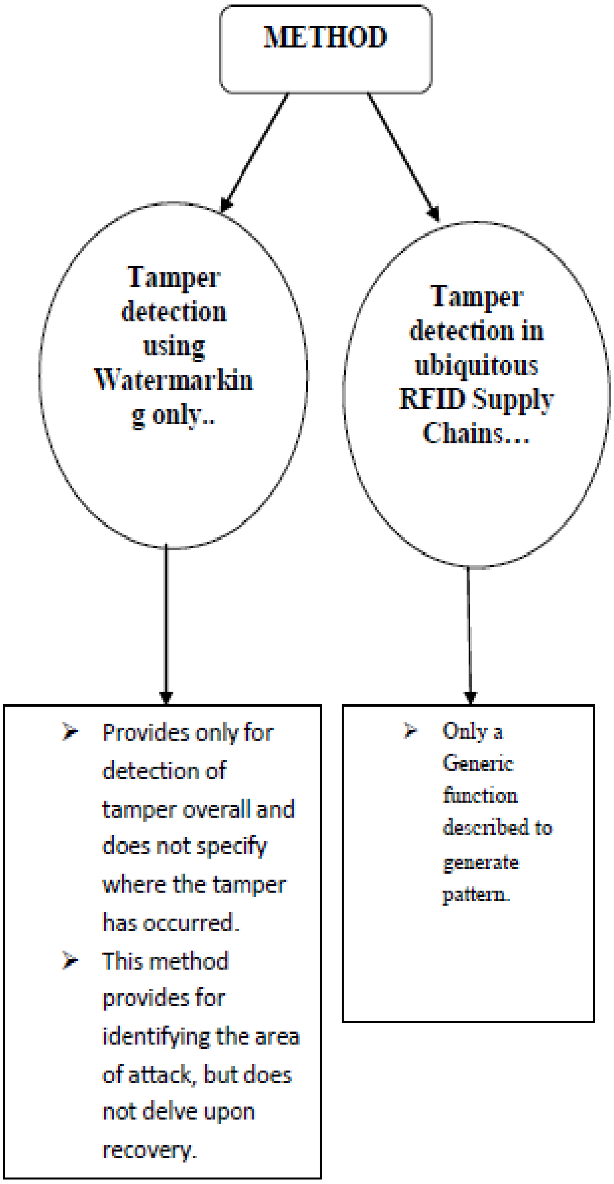
III. RELATED WORK

To address the tampering problem in RFID, concept of fragile watermark is introduced by Vidyasagar Potdar et al. [8] Using fragile watermarking whether the RFID tag is tamper or not is detected. The data of EPC manager and the Object class are combined to form a Bit String which undergoes chaotic hash function to generate an 8 bit watermark that is embedded in the serial number field. Using 8 bit watermark, we can generate 2^8 =256 pattern of watermarks. When the number of tags increases to more than 256, there is a possibility of the repetition of the watermark that is generated. This watermark generated are embedded in the serial number of the tags which contains 36 bits out of which 8 bits are reserved for watermark embedding. Thus watermark computed with tampered tag data may match with embedded watermark and tag can be validated as untampered tag.

Use of reserved memory in the tag for 32 bit kill and/or access passwords to embed the watermark generated by taking inputs from H, EM, OC and SN is proposed in [9].

Going through literature, we found some issues in earlier implemented tamper detection projects are as follows [10].

TITLE	**Recovering and Restoring Tampered RFID Data using Stenographic Principles**	**A Watermarking Based Tamper Detection Solution for RFID Tags**	**Tamper Discrimination in RFID tags using Chaotic Watermarking**
CONTENT	approach to embed secret pattern inside RFID Serial Number Partition to recover tampered data in Object Class	Embedding a watermark in RFID to detect tampering on any of the data fields of the tag.	Chaotic Watermarking is applied to RFID tags. This provides for Tamper detection as well as discrimination



A. Watermark generation using Choatic and hash function

- The embedding algorithm begins by selecting a set of one way functions F {f1, f2, f3}.
- Each one way function is applied to the values within the RFID tags partition to generate a secret value as shown[11]
- This secret value is then embedded at predefined location within the Serial Number partition by appending it to the original Serial Number Value (*SNorg*)to generate the appended Serial Number (*SNapp*)[12].

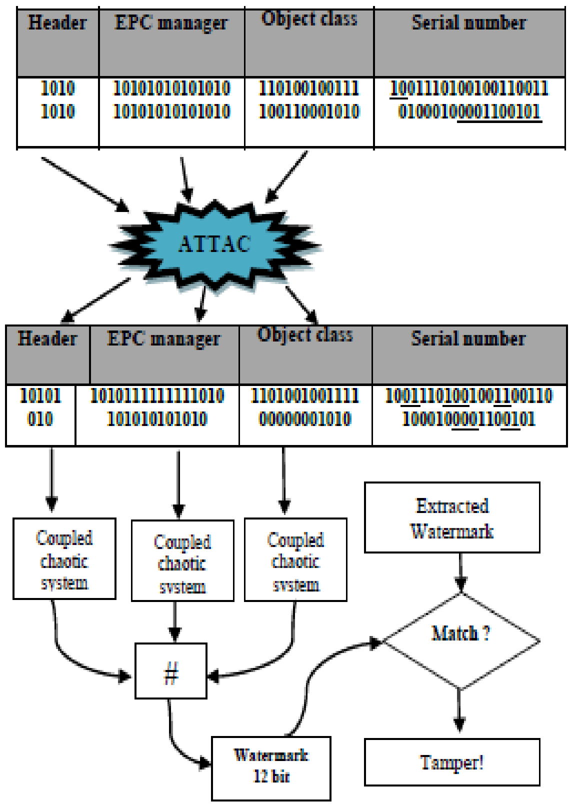


Fig: Tamper Detection

STEP 1: chaotic sequences are taken as the keys for encryption.

STEP 2: Map 8 bits of header, anterior 14 bits of EM, latter 14 bits of EM, anterior 12 bits of OC, latter 12 bits of OC as decimal fractions,d_1,d_2,d_3,d_4,d_5 respectively.

$d1 = b7 \times 2^{-1} + b6 \times 2^{-2} \ldots. b0 \times 2^{-8}$

STEP 3: For the length of Header is 8 bits, when header is Tampered, d1 is variational.

STEP 4: Use d_1 as the initial value of (1) will generate various chaotic sequences.

STEP 5: The sequence is converted to binary and any 2 bits from it is designated as W_1.

STEP 6: The EM is divided into two parts and each part is Mapped into two decimal fractions d_2 and d_3.

STEP 7: Since the length of each part is 14 bits, when each tampered, d_2 and d_3 will be variational.

STEP 8: d_2 and d_3 are used as initial condition for (1) and (2) respectively and any 5 bits from the obtained binary sequence is taken as W_2.

STEP 9: Similar method described above is used to generatewatermark W_3 for OC

STEP 10: Connect W_1, W_2 and W_3 to form final watermark W_f.

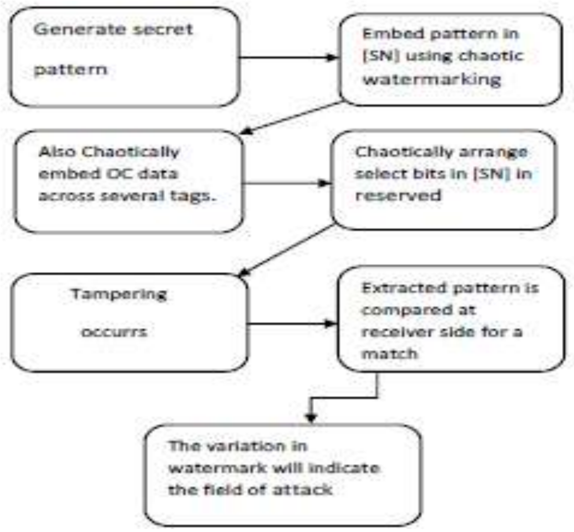


Fig. Schematic diagram of embedding watermark

Partition	Function	Secret Value
EPC Manager (EM)	1	A= ()
Object class (OC)	2	B= ( )
	3	C=

B. 12 bits and its advantages:

With 8 bit watermark, we can have maximum 2^8 =256 watermark patterns. So appearance of repetition of watermark generated, when tag number exceeds 256, is but natural. So, probability is there that even if some bits of EM or OC are tampered still same watermark pattern as that of original tag is generated and tag is finally approved as un-tampered tag!!

Here we increase watermark bits to 12. With 12 bits watermark, we can have 2^{12} = 4096 watermark patterns so we can have more number of secret patterns. We cannot further compromise with SN part of Tag, so limit to 12 bits only. SN here will be limited to 24 bits instead of 28 bits as with 8 bit watermark, which can still be acceptable[13].

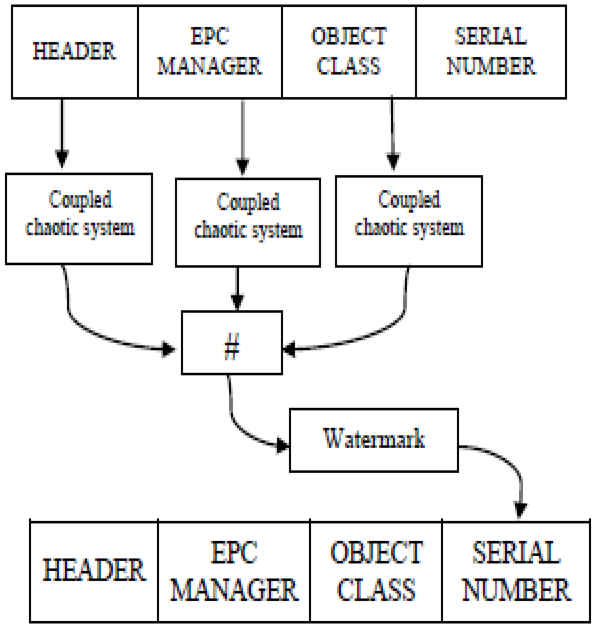


Fig: Basic Embedding

IV. CONCLUSION AND FUTURE WORK

Using this technique we can detect HEADER, OC, EM, SN. Also we are using 12 bits instead of 8 bits because of this more secret patterns can be generated. Main idea behind the project is that instead of finding fewer solutions we are generating improvised technique of tamper detection using sum chaotic sequence, hash functions. In future, if more bits are reserved for the secret pattern, the probability of repetition is negligible.

REFERENCES

[1] M.R. Rieback,B. Crispo, and A. S. Tanenbaum, "the evolution of RFID security, " IEEE PerCom 06, pp. 62-69, January-March 2006.

[2] C.C.Tan and Q Li, "A robust and secure RFID based prdigree system" ICICS, 2006.

[3] Klaus Finkenzeller, RFID Handbook: Fundamentals andApplications in Contactless Smart Cards and Identification, 2003 John Wiley & Sons, Ltd. ISBN: 0-470-84402-7

[4] Z. G. Prodanoff, "Optimal frame size analysis for framed slotted Aloha based RFID networks," Comput. Commun., vol. 33, no. 5, pp. 648— 653, Mar. 2010

[5] C. Wang, M. Daneshmand, and K. Sohraby, "Optimization of tag reading performance in generation-2 RFID protocol," Comput. Commun., vol. 32, no. 11, pp. 1346-1352, July 2009

[6] EPC global Inc., "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz -960 MHz Version 1.4", 2008.

[7] Lukas Grunwald, "RFDump Can Hack RFID Tags", Available online: http://www. rfidgazette. org/2004/0 7/lukas grunwalds. htmlAccessed on Sunday, 29, October 2006

[8] Vidyasagar Potdar, Elizabeth Chang, "Tamper detection in RFID tags using fragile watermarking," International Conference on Industrial Technology, Mumbai, India, 2006, vol.12, pp.2846-2852.

[10] Ali Nur Mohammad Noman et al, "A Watermarking Based Tamper Detection Solution for RFID Tags" 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 978-0-7695- 4222-5/10 2010 IEEE DOI 10.1109/IIHMSP.2010.32 Juels, A.: RFID Security and Privacy: A Research Survey, An invited paper, IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, pp. 381394, February 2006.

[11] Spiekerman, S., Evdokimov S.: Privacy Enhancing Technologies for RFID - A Critical Investigation of State of the Art Research, IEEE Privacy and Security, 2009.

[12] Yamamoto, A.; Suzuki, S.; Hada, H.; Mitsugi, J.; Teraoka, F. \& Nakamura, O. A Tamper Detection Method for RFID Tag Data, IEEE International Conference on RFID, 2008, 51-57.

[13] Kishor T. Patil.; Dr. Santosh K. Narayan khedkar, SIG College of Engg, Navi Mumbai, Research Scholar: SGB Amravati University, An Improved Fragile Watermarking Method for Tamper Detection bitin RFID Tag.