

Process of reading and writing the tag of the motor vehicle electrical identification system based on the RFID technology

Wu ChangCheng¹ Liu DongBo² and Hu JiaBin³

¹ Traffic management research institute of Public Security Ministry, WuXi, JiangSu, China.
E-mail: dingsouqing@163.com Tel: +886-0510-85501522

² Traffic management research institute of Public Security Ministry, WuXi, JiangSu, China.
E-mail: bdbliu@vip.sina.com Tel: +886-0510-85501522

³ Traffic management research institute of Public Security Ministry, WuXi, JiangSu, China.
E-mail: its11117@163.com Tel: +886-0510-85501522

Abstract—As the development of the intelligent transport system, motor vehicle electrical identification system, based on the theory of radio frequency identification, is widely researched to strength the traffic management. The motor vehicle electrical identification system is mainly composed of the tag, the reader and other aspects. Usually, the vehicle information, including the license number, the traveler name, the identification number and other personal information, is stored in the tag. Considering the radio communication between the tag and the reader, the personal security may be destroyed if the vehicle information is leaked. Therefore, this paper introduces a new process about reading and writing the tag of motor vehicle electrical identification system. Firstly, it designed the structure about the storage of the tag, including the information security area, the controlling area and the information area. Then, it proposed the method about reading and writing each area. Experimental results show that the proposed method can satisfy the command needing of the traffic management.

I. INTRODUCTION

Radio frequency identification, a new non-contact automatic identification technology, uses the radio frequency signal to access the relevant data and identify the target automatically. The simplest radio frequency identification system includes the tag, the reader, and the antenna. The tag stores the information and the reader uses the radio frequency signal to communicate the tag [1]-[9]. Usually, the radio frequency identification system is mainly used in these aspects, such as the manufacture, the retail, the logistics, the medical, the identification, the military, the security, transportation, the food, the books, the animal, and so on.

Although the radio frequency identification is mostly used for logistics management, its application in the motor identification system is still far from enough mature. Recently, the motor vehicle identification system is mainly designed to identify the vehicle automatically by the radio signal at the frequency of 800-900M. As shown in Fig.1, the motor vehicle electrical identification system mainly included the tag, the reader and the antenna. The tag is mainly used to store the vehicle information, while the reader is mainly used to read and write the vehicle

information from and into the tag respectively. The antenna is mainly used to offer the energy for the tag and receive the radio signal for the tag.

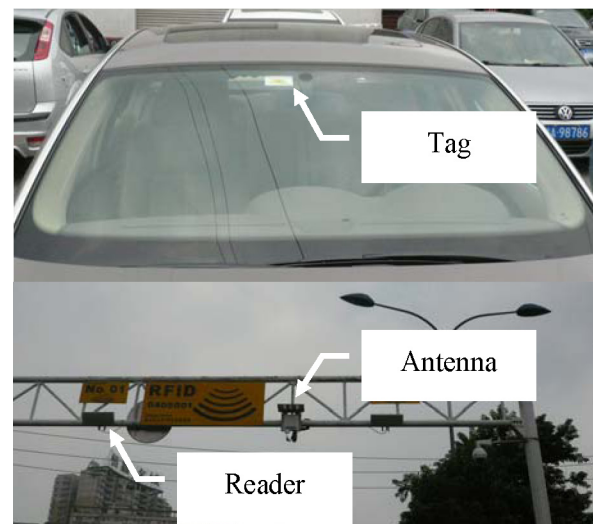


Fig.1 The main composed parts of the motor vehicle electrical identification system

Since the tag of the motor vehicle electrical identification system stored the vehicle information, such as the license number, the traveler name, the identification number and other personal information, the personal security may be destroyed if the stored information is leaked when the tag and the reader communicate each other. Therefore, this paper introduces a new process of reading and writing the tag of motor vehicle electrical identification system. Firstly, it designed the structure about the storage of the tag, including the information security area, the controlling area and the information area. Then, it proposed the method about reading and writing each area. Experimental results show that the proposed method can satisfy the command needing of the traffic management.

II. REVIEWING THE INFORMATION STORED IN THE TAG

As described in Ref.3, all information is stored in the memory of the chip in the tag. Seen from fig.2, the stored information mainly includes three parts, such as the tag information area, the controlling information area and the vehicle information area. The content about each area is described as following:

- (1) Tag information includes the assigned character, the chip manufacturer code and the serial number. The assigned character is represented as production of the chip according to different standards. The chip manufacturer code denotes the chip maker and the sequence number represents the different chip.
- (2) Controlling information includes the control command, the safety parameters and the identification password. The control command represents the operation of locking, inactivating, accessing the tag. The safety parameters represent the safety identification and safety communication, while the identification password is key, used to the access of chip storage.
- (3) Vehicle information includes the certification authority, the license plate number and other personal information. The certification authority includes the province code and the license authority code. The license plate number consists of numbers and letters, while the other related information refers to the demand of other application of vehicle information.

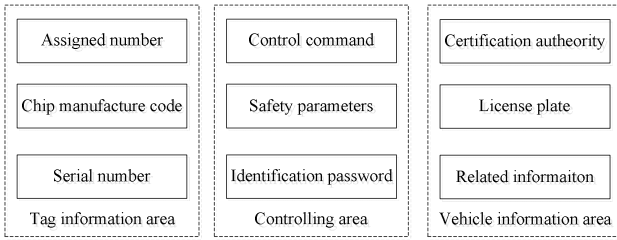


Fig.2 The information stored in memory of tag

III. READING AND WRITING THE STORED INFORMATION IN THE MEMORY OF THE TAG

A. Writing the tag information area

As described in fig.2, the tag information area stored such information, like the serial number, the assigned number, the chip manufacture code, and so on. Usually, the memory, used to store the tag information, can be written only once in the factory and cannot be rewritten after the factory.

As shown in fig.3, the whole steps about the writing the tag information area can be described as following:

- (1) Tag resets after entering the radio frequency field and gets ready for the inventory of the reader.
- (2) Tag verify the reader: if yes, goes to step 2; otherwise goes to step 6;
- (3) Reader verify the tag: if yes, goes to step 4; otherwise goes step 5;

- (4) Writing permission of tag information area: if writing is permitted, goes to step 5; otherwise goes to step 6;
- (5) Write tag information area: if succeed, update the tag information area; otherwise goes to step 6.
- (6) End.

Seen from the above discussion, we can see that the memory, stored the tag information, can be successfully written only after completing the above steps. At first, the tag obtains the energy from the antenna. Then, the tag and the reader verify each other. Other steps can go on only after they are successfully verified. At last, the tag information area can be updated only after judging it as the first writing and writing it successfully.

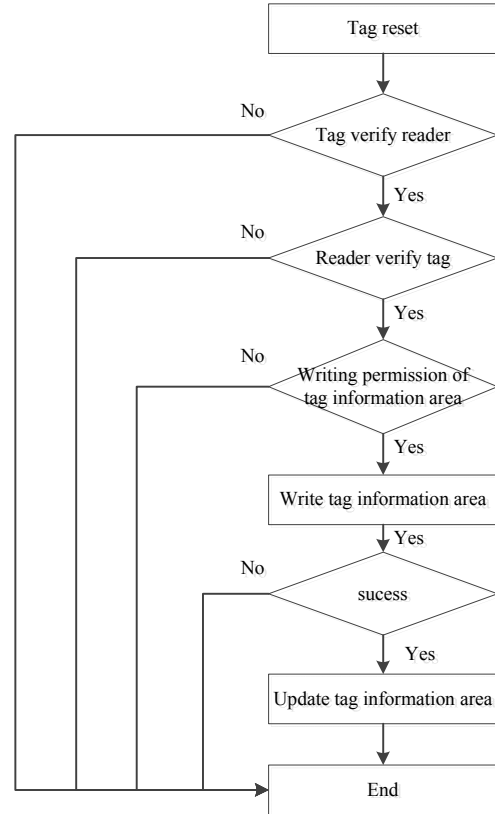


Fig.3 Steps about writing the tag information area

B. Reading the tag information area

Compared with the writing process of the tag information area, the reading process can be completed any time. As shown in fig.4, the whole steps about reading the tag information area can be described as following:

- (1) Tag resets after entering the radio frequency field and gets ready for the inventory of the reader.
- (2) Tag verify the reader: if yes, goes to step 2; otherwise goes to step 5;
- (3) Reader verify the tag: if yes, goes to step 4; otherwise goes step 5;
- (4) Reader read the tag information area: if read successfully, the tag returns the desired information; otherwise goes to step 5;

(5) End.

Seen from the above discussion, we can see that the memory, stored the tag information, can be successfully read only after completing the above steps. At first, the tag obtains the energy from the antenna to supp. Then, the tag and the reader verify each other. Other steps can go on only after they are successfully verified. At last, information in the tag information area can be obtained after the reader reading the tag successfully.

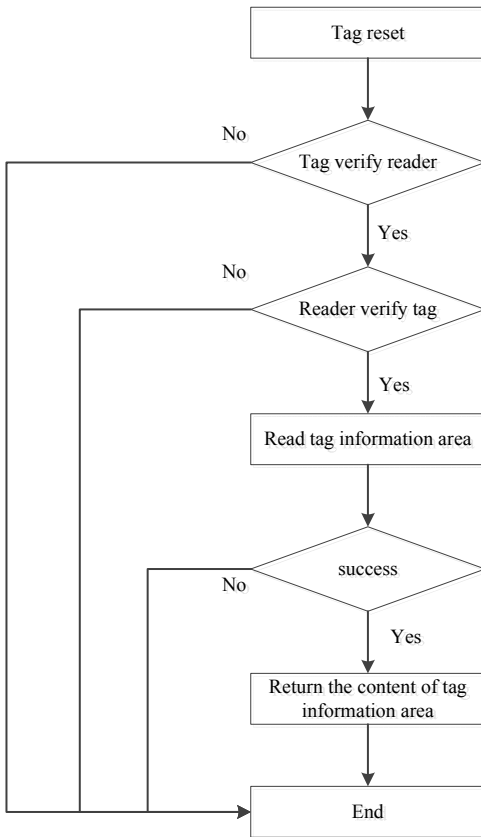


Fig.4 Steps about reading the tag information area

C. Writing the controlling area

As described in fig.2, the controlling information area stored such information, liking the control command, the safety parameters and the identification password.

As shown in fig.5, the whole steps about writing the controlling area can be described as following:

- (1) Tag resets after entering the radio frequency field and gets ready for the inventory of the reader.
- (2) Tag verify the reader: if yes, goes to step 2; otherwise goes to step 6;
- (3) Reader verify the tag: if yes, goes to step 4; otherwise goes step 6;
- (4) Writing permission of the controlling area: if writing is permitted, goes to step 5; otherwise goes to step 6;
- (5) Write the controlling areas: if succeed, update the controlling area; otherwise goes to step 6.
- (6) End.

Seen from the above discussion, we can see that the memory, stored the controlling information, can be successfully written only after completing the above steps. At first, the tag obtains the energy from the antenna to supp. Then, the tag and the reader verify each other. Other steps can go on only after they are successfully verified. At last, the controlling information area can be updated only after permission allowed and writing it successfully.

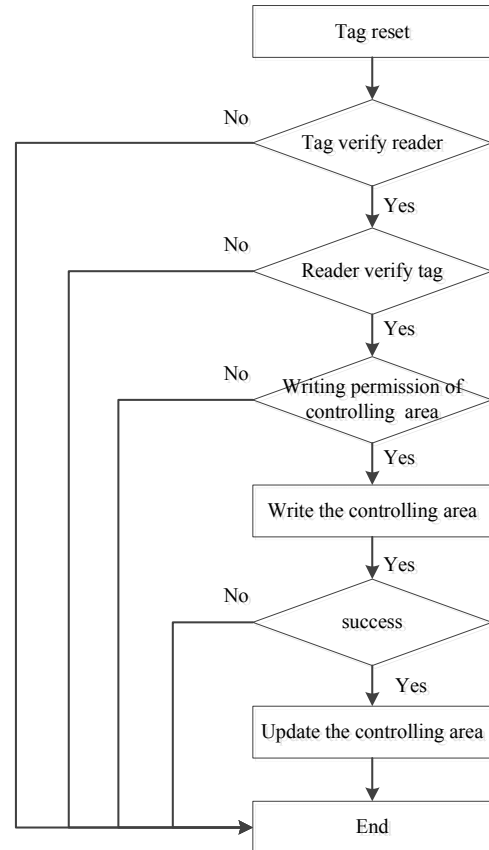


Fig.5 Steps about writing the controlling area

D. Reading the controlling area

As shown in fig.6, the whole steps about reading the controlling area can be described as following:

- (1) Tag resets after entering the radio frequency field and gets ready for the inventory of the reader.
- (2) Tag verify the reader: if yes, goes to step 2; otherwise goes to step 5;
- (3) Reader verify the tag: if yes, goes to step 4; otherwise goes step 5;
- (4) Reader read the tag: if read successfully, the tag returns the desired information; otherwise goes to step 5;
- (5) End.

Seen from the above discussion, we can see that the memory, stored the controlling information, can be successfully read only after completing the above steps. At first, the tag obtains the energy from the antenna to supp. Then, the tag and the reader verify each other. Other steps can go on only after they are successfully verified. At last, the information in the controlling information area can be

obtained by the reader after the read reading the tag successfully.

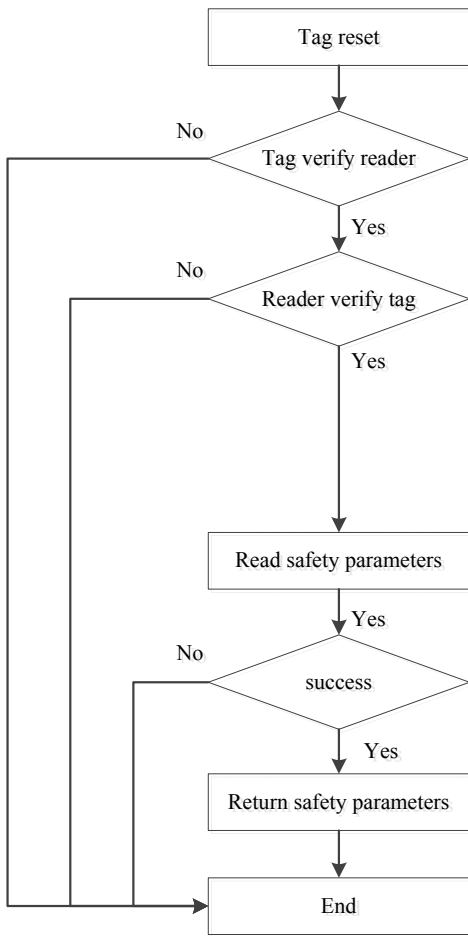


Fig.6 Steps about reading the controlling area

E. Writing the vehicle information area

As described in fig.2, the vehicle information area stored such information, liking the certification authority, the license plate number and other related information. Since the vehicle information area includes personal information, not all of the traffic management can use this information directly. Therefore, we proposed the way of authorization to meet this demand. Only the authorized user can write the vehicle information area.

As shown in fig.7, the steps about writing the vehicle area can be described as following:

- (1) Tag resets after entering the radio frequency field and gets ready for the inventory of the reader.
- (2) Tag verify the reader: if yes, goes to step 2; otherwise goes to step 7;
- (3) Reader verify the tag: if yes, goes to step 4; otherwise goes step 7;
- (4) Writing permission: if writing is permitted, goes to step 5; otherwise goes to step 7;
- (5) Writing authentication: if authorized, goes to step 6; otherwise goes to step 7;

- (6) Write information into the vehicle information area: if succeed, update the vehicle information area; otherwise goes to step 7.
- (7) End.

Seen from the above discussion, we can see that the memory, stored the vehicle information, can be successfully written only after completing the above steps. At first, the tag obtains the energy from the antenna to supp. Then, the tag and the reader verify each other. Other steps can go on only after they are successfully verified. At last, the vehicle information area can be updated only after writing permission allowed, writing authorized, and writing it successfully.

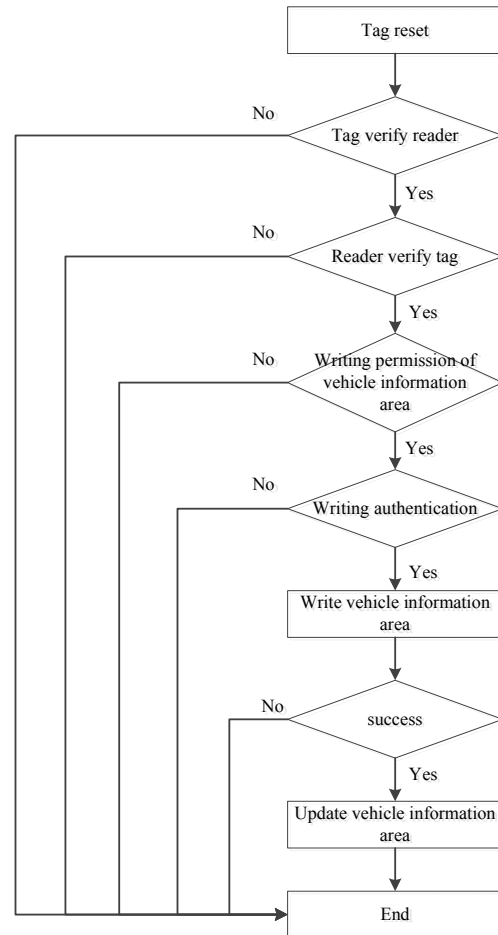


Fig.7 Steps about writing the vehicle information area

F. Reading the vehicle information area

Liking the process of wring the vehicle area, only the authorized user can read the vehicle information. As shown in fig.8, the steps about reading the vehicle area can be described as following:

- (1) Tag resets after entering the radio frequency field and gets ready for the inventory of the reader.
- (2) Tag verify the reader: if yes, goes to step 2; otherwise goes to step 7;
- (3) Reader verify the tag: if yes, goes to step 4; otherwise goes step 6;

- (4) Reading permission: if reading is permitted, goes to step 5; otherwise goes to step 7;
- (5) Writing authentication: if authorized, goes to step 6; otherwise goes to step 7;
- (6) Reader read the tag: if succeed, the tag return the desired information; otherwise goes to step 7.
- (7) End.

Seen from the above discussion, we can see that the memory, stored the vehicle information, can be successfully written only after completing the above steps. At first, the tag obtains the energy from the antenna to supp. Then, the tag and the reader verify each other. Other steps can go on only after they are successfully verified. At last, the vehicle information area can be obtained by the reader only after reading permission allowed, reading authorized, and reading it successfully.

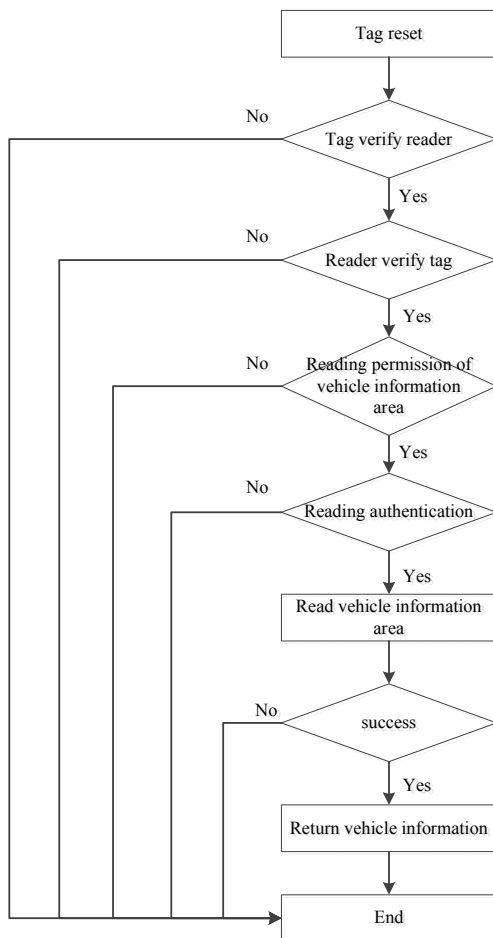


Fig.8 Steps about reading the vehicle information area

IV. CONCLUSION

This paper introduced the process of writing and reading the information in the memory of the tag in the motor electrical identification system. Considering the information in the tag information area, the controlling information area and the vehicle information area, this paper also describes the

writing and reading process in each area. Considering the personal information in the memory of the tag in the motor electrical identification system, the proposed authorized based method can solve this problem, satisfying the need of each traffic management.

REFERENCES

- [1] Sarma S. E., Weis S. A., Engels D. W.. Radio frequency identification: Secure risks and challenges[R].RSA Laboratories Cryptobytes , 2003,6 (1):2-9.
- [2] Weis S.A.,Sarma S.E.,Rivest R.L.,Engels D.W. Security and privacy aspects of low-cost radio frequency identification systems[A]. Proceedings of the 1st International Conference on Security in Pervasive Computing[C]. Berlin:Springer-Verlag,2004:50-59.
- [3] Weis S.A.,Sarma S.E.,Rivest R.L.,Engels D.W. Security and privacy aspects of low-cost radio frequency identification systems[C]. Proceedings of the 1st International Conference on Security in Pervasive Computing. Berlin:Springer-Verlag,2004:201-212.
- [4] Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita. Cryptographic approach to “privacy-friendly” tags[C]. In RFID Privacy Workshop, MIT, MA, USA, November 2003.
- [5] Jones AK. Password Authentication with Insecure Communication [J].Communications of the ACM, 1981,Vol.24(11): 770-772.
- [6] Ouyang CQ, Wu JX, Li ZY, Huang SY. An Enhanced Security Authentication Protocol Based on Hash-Lock for Low-cost RFID[C]. The 2nd International Conference on Anti-counterfeiting, Security and Identification, 2008: 416-419.
- [7] Lee SM,Hwang YJ,Lee DH,Lim JI.Efficient Authentication for Low-Cost RFID Systems[A]. ICCSA 2005,volume 3480 of Lectures Notes in Computer Science[C].Berlin:Springer-Verlag,2005: 619-627.
- [8] Henrici D, Müller P. Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. Pervasive Computing and Communications Workshops, 2004: 149-153.
- [9] Yang J, Park J, Lee H, Ren K, Kim K. Mutual Authentication Protocol for Low-cost RFID[C]. Ecrypt Workshop on RFID and Lightweight Crypto, Graz, 2005.