IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 5, 2019, accepted July 23, 2019, date of publication August 5, 2019, date of current version August 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2933236

Study on the Anti-Theft Technology of Museum Cultural Relics Based on Internet of Things

ZELIANG LIU[1,2], MIN WANG[2], SHIKAI QI[1], AND CHANGCHUN YANG[1]
[1]School of Electronic Engineering, Jiujiang University, Jiujiang 332005, China
[2]School of Computer Science, Wuhan University, Wuhan 430072, China

Corresponding author: Min Wang (min.whu@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 511667009 and Grant 61563023, in part by the Science and Technology Project of Jiangxi Provincial Health Commission, China, under Grant 20185533, and in part by the Humanities and Social Sciences Research Project of Jiangxi Province under Grant JC17122.

ABSTRACT With the advancement of society, the museum has exhibited more and more cultural relics, the number of visitors has also increased rapidly, and more and more criminals have stolen cultural relics. The traditional anti-theft methods cannot completely block their pace. This paper proposes a museum anti-theft scheme based on the Internet of Things (IoT) technology, which identifies whether the cultural relics are within the safe range through the passive RFID readers/writers. Once stolen, the cultural relics will leave the effective RFID identification range, which results in immediately alarming, then the system starts the anti-theft plan. The method is free from the drawbacks of the traditional infrared anti-theft, door magnetic detection and the like, the proposed anti-theft method monitoring has the immediacy and the safety factor is higher. Finally, in this paper, hardware circuit designs, software development and a series of tests are carried out to achieve the desired results.

INDEX TERMS Internet of Things, anti-theft, RFID, museum.

I. INTRODUCTION

With the improvement of people's cultural life, art galleries and museums around the world have become the first choice for people to travel. By the beginning of 2019, the total number of museums in our country reached 5,136 [1]. For a long time, museums have always regarded nonprofits and public welfare as a social consensus. In many countries, museums must be open to the public free of charge. In 2018, the National Museum held more than 20,000 exhibitions, nearly 1 billion people walked into the museum, and visiting the museum became a way of life. This makes the cultural relics in the museum also be a part of the illegal elements. The theft of artifacts is something that people don't want to see [2]. To ensure the safety of the museum, the museum will develop various cultural relics protection measures to ensure the safety of them. However, even in this case, theft is still widespread.

The most widely used anti-theft technology is the burglar alarm, which has been applied in various industries. In the financial industry, like banks, ATM machines and other places, the installation of anti-theft alarm devices can minimize the occurrence of criminal cases such as robbery. In military areas, most information needs to be effectively kept secret [3], and anti-theft systems can detect whether suspicious individuals who are trespassing. In places with high traffic flow such as train stations and schools, by adopting face recognition technology, criminals and suspicious persons in the blacklist can be alerted. This efficient method can curb the occurrence of violent incidents and criminal incidents in order to protect the safety of people's lives and property [4], in addition, burglar alarm products are universally applied to the community to protect the property of community residents and uploaded to the police as evidence.

Commonly used traditional anti-theft products include infrared microwave detector, glass break detector, microwave target motion detector, and door magnetic detector. The infrared microwave detector is an emergency alarm device based on the working principle of infrared and microwave. Compared with other traditional anti-theft alarm products, infrared microwave detectors only generates alarm signals when it simultaneously trigger infrared detector and microwave detector [5]. In order to meet different needs, industrial infrared microwave detectors are equipped with

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

various signal devices to detect the degree of damage at different distances. The glass break detector is mainly used to detect the sound of glass breakage. The glass-crushing detector has a limited sound capture range, it can only detect the high-frequency sounds that come from the broken glass, and not for detecting ordinary glass vibration. The microwave target motion detector is a detector for detecting the Doppler shift of high frequency radio waves and it primarily used in open spaces, such as square spaces. Compared to infrared waves detector, microwave target motion detector owns very high frequency radio waves of very short wavelengths, which means that microwaves are easily reflected by other objects. The frequency shift of the incident and reflected waves can be used to detect intrusions. The door magnetic detector is not a very rare burglar alarm product. It consists mainly of an active part and an output part, which form the switch of the detector. The gap between the movable part and the output part is very small, which ensures the alarm sensitivity of the door detector.

At the earliest time, the means of museum was locked. Now we can see in the Forbidden City many unopened exhibition areas are hung with a big lock. However, due to the continuous development of society, the most conventional locking method has many limitations [6], and thieves can easily open the lock. Later, the high-tech system of the museum anti-theft system is sound waves. With the continuous development of the electronics industry, people can detect various types and frequencies of sound waves through electronic devices, so the sound-proof anti-theft devices come into being. In 1960, China introduced this equipment to the National Palace Museum for the first time. The advantage of this device is that even if the thief carefully implements the theft, the system will alarm if the detected frequency is offset during the detection process. However, the shortcoming of this system is that it may receive interference from external physical information, such as thunder and rain, talking sounds, etc., and it is easy to be touched [7]. In recent years, cameras have been installed in major museums to detect collections in venues and to employ the image recognition technology for theft prevention.

II. INTERNET OF THINGS TECHNOLOGY CHANGED THE ANTI-THEFT MODE

However, since common optical cameras cannot record image information at night without a light source, an infrared detector is added to the camera. Because of the temperature of the human body is higher than the other object, the detecting device can find the thief who enters the monitoring area at night, and performs signal processing after receiving the signal, and an alarm occurs. However, this system needs to arrange security for viewing video, which not only requires a lot of manpower, but also monitors the picture easily. The infrared alarm can also be affected by the temperature adjustment devices such as air conditioners. If the criminals block the probe with a red cloth, the alarm device will not work [8]. As the IoT technology gradually mature, the application of IoT technology to museums for theft prevention has become a research hotspot and encounters many challenges.

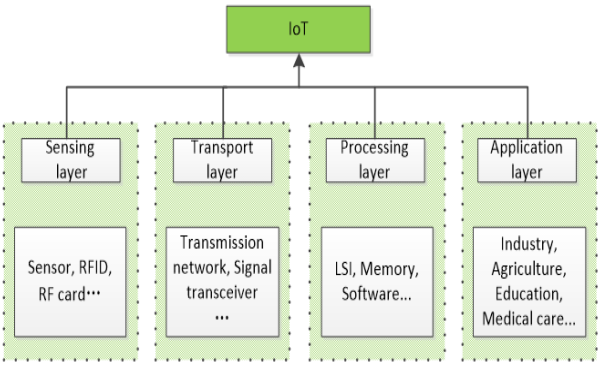


FIGURE 1. IoT architecture based on four components.

IoT is an extension of the Internet that connects physical devices with daily supplies. These devices are embedded in electronic devices, Internet connections, and other forms of hardware such as sensors, which communicate with others utilize the Internet or remote monitoring [9]. It is a network of connected objects, taking advantage of the network, it combines sensor technology, computer network technology and automatic control technology to achieve communication between objects. The IoT device structure can be divided into four parts of the sensing layer, the transport layer, the processing layer and the application layer. Its architecture is shown in Figure 1.

As the definition of the IoT has evolved into a multi-technology, real-time analysis, machine learning, commodity sensors and embedded systems integration. Traditional areas such as embedded systems, wireless sensor networks, control systems and automation (including home and building automation) contribute to the IoT [10]. With the rapid development of big data, blockchain, artificial intelligence, 5G and other technologies, the IoT has been rapidly developed in various industries, which has influenced all aspects of people's lives [11]–[17].

As an IoT technology, RFID has been widely used in various industries. It is also considered as an eminent enabling technology for the realization of ubiquitous monitoring in IoT [18], [19]. RFID is a key building block for future IoT world, where sensors are connected for pervasive monitoring and control [20], [21]. RFID has been extensively used in various fields at home and abroad, including access control management, security control, document management, animal tracking, food and drug management, baggage management, commercial automation systems, commodity supply chain management, and logistics management. For example, RFID technology is widely used in Canada to track museum exhibits, manage attendance, manage warehouse storage, track official documents, manage billing routes, collect data processing, and more. Several research efforts in the past few years have made the passive RFID beyond simple barcode replacement but to enhanced RFID tags. These trends

combine the potential of WSN and RFID technologies to implement identification, sensing, arbitrary processing, data logging, and actuation functionality [22]–[29]. At present, China's RFID technology is the mostly used in logistics and warehousing [30].

Europe and the United States have the most extensive research and practical experience in the field of RFID, but they lack the industry standards that can provide a wide range of applications. RFID technology is currently a hot topic of research, which can locate the location of the items that users need. Places like libraries and parking lots in more places where RFID is used [31]. An RFID reader is installed at the entrance and exit where the system can monitor the precise position of the objects with the RFID tag at any time. The essence of this system is equivalent to arranging security guards at the entrance and exit. When using this system to find the specific information of an object, you only need to scan the RFID tag on the object to view it on software.

Based on the RFID technology, museum ticketing and visitor management systems have been come into being. Through this system, the museum will be managed more efficient and orderly organizated. In addition to satisfying the basic ticket sales function, it can also capture the behavior of tourists [32], carry out statistical analysis, and implement cultural values in a targeted manner. Promotion services are in line with the characteristics of the museum. Specifically, the following three requirements should be satisfied, 1. One person with one vote, verification visit, and free chance to visit the museum's basic display. 2. The real-name system visitors must provide the necessary personal information during the ticket booking process, and hold valid identification documents during the ticket purchase and admission process to prepare for the services such as ticket checking, information collection and selection. 3. According to the scale and openness of the construction site, the best reception capacity and maximum reception capacity should be fully considered, as well as the comfort and safety of the visit. At the same time, we can set the maximum reception capacity of the museum according to the daily reception capacity of the museum and the special travel time.

In the creation of interactive museums, domestic and foreign scholars have basically reached a consensus on education and business, and put forward more innovative applications and research trends. Falken security network's industry management has many practical and innovative practices [33], which detailedly describes how to use RFID management to quickly locate more than 15,000 exhibits in museums or galleries within two hours.

Based on research about the theory and practice of RFID museums at home and abroad, it has been found that the interactive museum of RFID technology combines the preferences and personality of tourists, this new method changes the impression of museums in the past. Europe and the United States are primarily conducted on private companies, while Asia is guided by government policies. This new type of museum is well appeared by investors and visitors, not only because of the low investment, but also because they can improve the individualized learning experience of visitors and enable them to participate fully in the museum. However, there are still many issues that need to be discussed in detail. For example, what kinds of RFID technology is suitable for museums, what kinds of tourist attractions, what kinds of tourists and exhibition tracking procedures are enough, and so on. This is not only a technical difficulty, but also a difficult decision at the economic level [34].

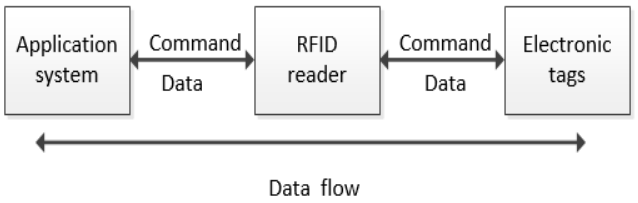


FIGURE 2. Process of the RFID data transmission.

RFID opens the door to a series of exciting self-service museums that employees effectively manage the transportation and display of exhibits. Users can get access to multimedia information of interest about individuals through simple handheld device scanning and RFID-enabled personal digital assistant information. Under the guidance of high-tech missions, a refreshing museum is open to the public, and RFID will be widely recognized by the public. The new technology museum must inject RFID. The museum industry should share clues, expand ideas, face future challenges, and create the expected digital vision.

III. THE OVERALL ARCHITECTURE OF ANTI-THEFT SYSTEM

Radio Frequency Identification (RFID) is a technology that uses remote storage and retrieval of data, which provides an identity code to monitored objects [35]. In general, it consists of an RFID reader, antenna and RFID tag. The unique identification code table is stored as an identity code in the RFID tag, while the other information of monitored objects are also stored in the tag, depending on the specific objects and storage size.

In a typical application, the RFID reader queries the tag in the interrogation zone to transmit the identification data. The process of data acquisition, data processing and data transmission are performed in real time, as shown in Figure 2.

Normally, the owner will only realize that the objects are missing when the objects are no longer in view [36]. The anti-theft system required by the user does not rely on the naked eye to protect the object and prevent lost. Instead, it should be automatically monitored by some technical means to remind the user in real time, and the detailed situation recorded in the monitoring system for tracking can achieve prevention. Items such as art, museum artifacts, and rare books are rarely moved in the display, and the RFID reader can be used to identify whether the item has moved or not.

The proposed anti-theft system is mainly composed of a PC, a RFID reader and an electronic tag, as shown

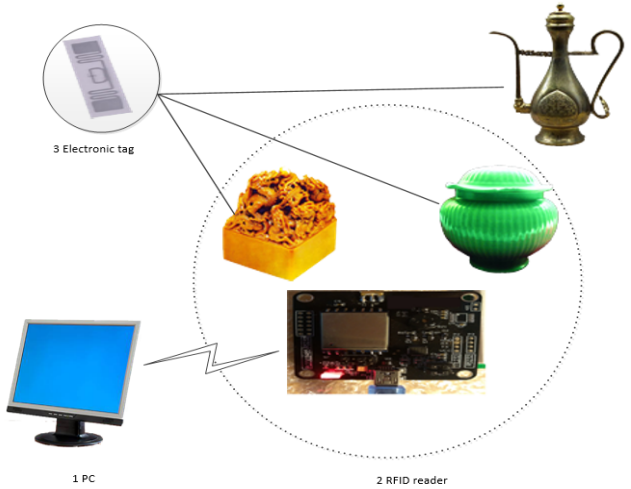


FIGURE 3. Composition of the RFID system.

in Figure 3. A corresponding application is installed on the PC for monitoring and controlling the data of the RFID reader. The electronic tag is flexible and can be installed on various artifacts without damaging the basic attributes and functions of the artifact. It communicates wirelessly with the RFID reader. The reading range of the RFID reader can be reasonably set according to the power size and the application program. The information of each electronic tag is read at regular intervals to detect whether the electronic tag is within its range, so as to determine whether an alarm signal needs to be emitted.

The RFID reader is mainly composed of a controller unit and a radio frequency transceiver module. RFID tag consists of a chip and a coupling element, each tag has a specific code that is attached to the surface or inside of the object and can be identified. There are two memory areas in the tag, one is to store the ID. The other is a data area for storing user information data, and such data can be modified and deleted.

Nowadays, since the inside of the electronic tag is basically made by a printing process, an antenna is manufactured. As a result, the overall manufacturing process cost of the label has been greatly reduced. When the electronic label can realize flexible folding and bending, it means that the application range of the electronic label will be more widely expanded in many fields.

The new flexible electronic tag adopts its light and thin, versatile features and response mechanism to embed the electronic tag in the interlayer of the important target or the package [37], and simultaneously install the tag positioning receiver in the storage area of the important target. When both the locator and the tag are within the valid working range of the acknowledgment signal, the system defaults to the safe state if the communication response matches correctly after the data link match. It will automatically alarm when it is detected that the security target is abnormally moved (beyond the effective response range), or the response signal suddenly disappears (abnormal interruption), or the package of the built-in electronic tag is artificially destroyed, or the circuit system built in the package interlayer is destroyed (normal communication).

TABLE 1. The difference between linearly polarized antenna and circularly polarized antenna.

Performance characteristics	Linearly polarized antennas	Circularly polarized antennas
Sending method	Sending in a linear manner	Sending in a circular spiral
Electromagnetic field	Linear beam, unidirectional Electromagnetic	Circular spiral beam, multi-directional electromagnetic
Directionality	Strong	Weak
Reading range	Narrow and long	Width
Reading distance	Far	Nearby
application	Clear	Unclear

At the same time, the target object is automatically positioned. The alarm and positioning information are sent to the manager or the user in synchronization, then the position tracking is started in real time. The user or the administrator can receive and view the specific location information of the security objects at any time through the computer management terminal, so as to make subsequent processing decisions. If there is no abnormal location migration or sudden interruption of communication, the main role of the system at this time is to perform location monitoring and inspect the targets with important value.

IV. SYSTEM PROGRAM DESIGN

The core hardware of this system is the card reader module, which contains the JRM2030 chip. Its operating frequency is 840-960MHz and adopting EPC C1 GEN2/ISO 18000 −6C protocol, the maximum output power is +27dBm, the reading range can be adjusted according to the output power. The system functional block diagram is shown in Figure 4.

As shown in Figure 5, the core module circuit diagram. The module's UART serial port is TTL3.3V. If you use PC serial communication, since the serial port of the module is TTL3.3V, you need to use MAX3232 for level conversion.

Before designing the system software, it is necessary to clarify the tasks and functions of the system as a whole, because the software function of this system fundamentally determines the role of the system and the development trend. The card reader module is used to scan the electronic tags of all the cultural relics in the museum. As long as the

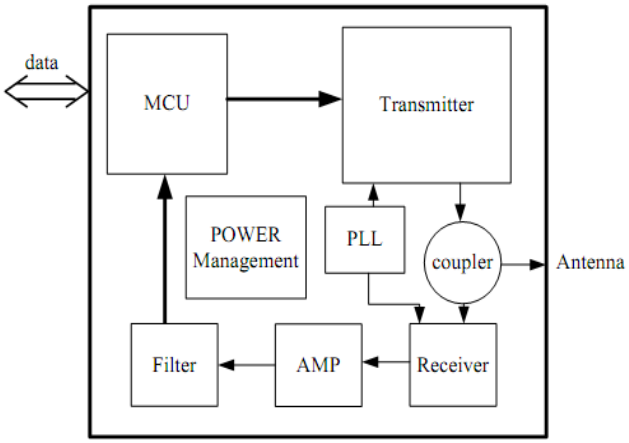


FIGURE 4. Functional block diagram in anti-theft system.

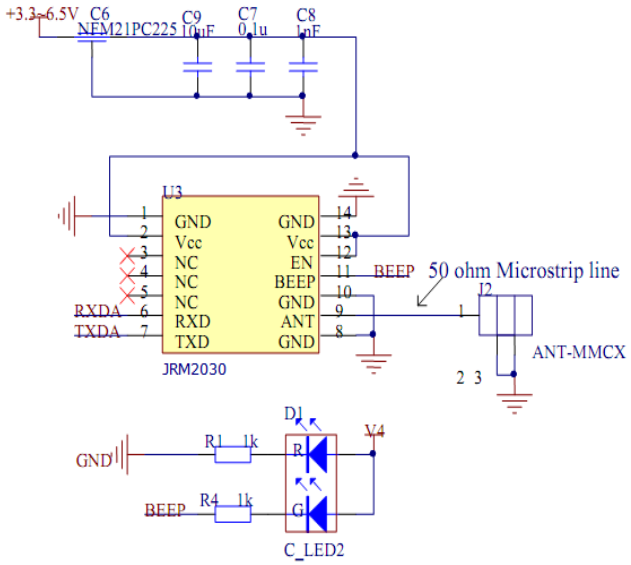


FIGURE 5. Core module circuit diagram.

devices are not within the recognition range of the ultra high frequency RFID system, the system will recognize devices are stolen.Then the system will sent sound and light alarm information, at the same time the camera system is activated to capture a snapshot. Finally, the system will close the gate, block the entrance exit and channels. By the means of concealment of RFID recognition, the response speed is fast and the anti-theft effect is better.

The core technology of the museum anti-theft module is the rapid identification of electronic tags and the process of reading data by RFID readers. The main advantages of the system are two aspects, firstly, the use of RFID readers for identification, wide range of reading tags, distances up to 5 meters, which can achieve a wide range of anti-theft field; secondly, the security of the anti-theft system is high Real time is strong. Once the museum equipment is removed from the unrecognized area of the RFID system antenna, it is considered to be in danger of losing the device

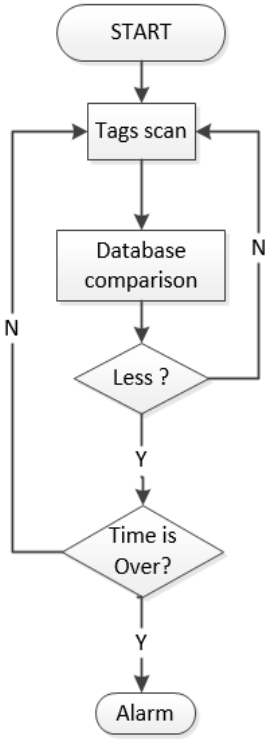


FIGURE 6. Museum anti-theft system flow chart.

and the system immediately alerts. Traditional museum theft just uses a device to inspect people at the entrance to the museum. An alarm is issued when the device is accidentally removed from the museum entrance and exit [29]. If the item is destroyed or stolen, but it has not passed through the museum entrance and exit, it will not have an alarm message. These kinds of museum anti-theft has certain limitations.

In this design scheme, by arranging the RFID system around the cultural relics, once the RFID system recognition range is left, the alarm starts, which has more comprehensive considerations. To this end, the anti-theft mode of the cyclic scan electronic tag is designed, and the time required to complete the whole anti-theft function is determined according to the number of museum devices. During this time, if the corresponding device is scanned multiple times and the corresponding device is not detected. The alarm processing starts. Figure 6 is a flow chart of the program design of the museum anti-theft system.

In the RFID application system, reader/writer is connected to communication controller (or PC) in application system via RS232 port. The reader/writer receives command from the controller, and returns the command execution result to the controller. Therefore, we call the data communication packet which sents from the controller to the reader as a command packet, and call the data communication packet which sents from the reader to the controller as a return packet. During communication, the host computer sends commands and parameters to the card reader module, and the card

TABLE 2. Firmware Instructions. Co:Command, P:Parameter, C:Checksum.

Header	Type	Co	PL(MSB)	PL(LSB)	P	C	End
AA	00	07	00	01	01	09	8E

reader module returns the status and data of the command execution results to the host computer. The reader receives the command and executes the command until the reader completes the execution of the command before receiving the next command. If a command is sent to the reader during a command execution by the reader, the command will be lost.

In the data stream sent by the host, the transmission interval between two adjacent bytes must be less than 15 milliseconds. In the process of transmitting the host command data stream, if the adjacent character interval is greater than 15 ms, the previously received data will be discarded invalid data and then re-received from the next byte. When the reader receives the correct command, it will return a response to the reader within a range that does not exceed the query time (not including the data sending process, which is only the time the reader executes the command).

In the process of response data sent by the reader, the whole communication process between adjacent bytes is that the host sends a command to the card reader, and waiting for the card reader to return a response. After the reader receives the command, it begins executing the command and then returns a response, after which the host receives a response from the reader.

In this system, EPC electronic tags are also an important component. It is a passive tag that uses modulated scatter to transmit data and uses the carrier of the reader to modulate its own signal. The reader can scan and read the tag information at regular intervals (user-defined), decodes it and sends it to the computer system for data processing. Logically, the tag memory is divided into four storage areas, each of which can be composed of one or more memory units. (1) EPC, EPC number is stored in the EPC area. This reader specifies that it can store up to 15 words of EPC, readable and writable. (2) TID,TID stores the ID number set by the label manufacturer. Two ID numbers of 4 words and 8 words are readable and not writable. (3) User, the user area is different from the manufacturer area. Inpinj's G2 tag has no user area, and philips has 28 words. Readable and writable. (4) Password, the first two words in the password area are the KILL password, and the last two words are the Access password. Readable and writable.

Setting the firmware instructions in the underlying MCU program. The firmware instruction consists of frame type, instruction parameter, instruction code, frame header, check code, end of frame and instruction data length, all those are expressed in hexadecimal. some of the defined firmware instructions is shown in Table 2.

FIGURE 7. Monitoring settings.

Each instruction frame has a corresponding response frame. The response frame indicates whether the instruction has been executed. According to the read conditions, the microcontroller in the reader module independently transmits the same number of notification frames to the host. When the reader reads the tag, it sends a notification frame; when the reader reads multiple tags, it sends multiple notification frames.

For application development, we use QT Creator to develop the implementation, as shown in Figure 7. The anti-theft software mainly includes user login, monitoring settings, communication parameter settings, monitoring display, user management and other main functional modules. When it is detected that the tag is not within the setting range, the alarm device is triggered to perform an alarm.

Through the design and development of the hardware circuit, the realization of the software, the establishment of the network connection, the overall function for debugging and verification, has achieved the expected results.In Figure 8, the experimental circuit board was developed is shown.

V. EXPERIMENT AND DISCUSSION

In the experiment, we also carry out some software function tests. The software and hardware connections are normal, all functions can be realized. The interface is friendly and the expected results are achieved. Test contents and results are shown in Table 3.

At the same time, the reading or writing distance of the card reader is simply tested. During the test, the power of the card reader is set to the default value of 20dbm, when the distance and angle of the tag are changed, the data is recorded. At zero offset angle, the test of the reading rate at different distances is shown in Figure 9. Data analysis shows that the reading rate of the tag decreases as the distance increases. Between 0 and 3 meters, the label reading rate is high, there is no big change, which is the reliable range of application. When the

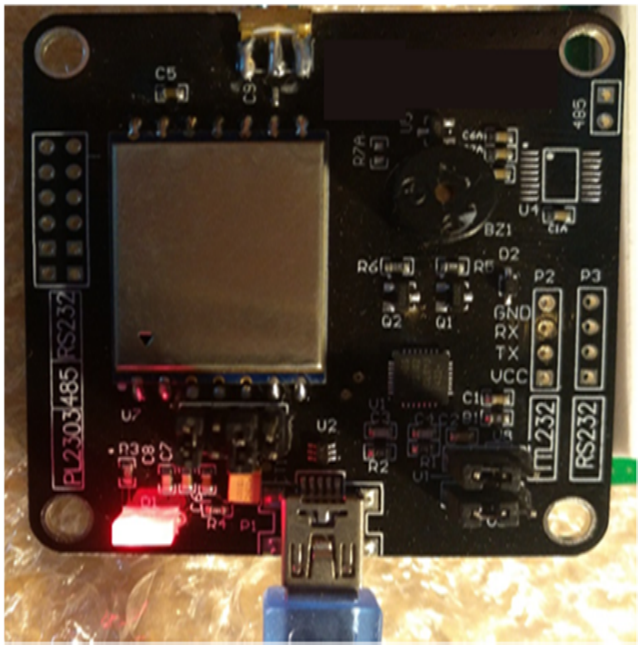


FIGURE 8. Experimental board.

TABLE 3. Software function tests.

No.	Function	Result
1	Software installation, uninstallation	Complete
2	Software interface display	Normal
3	Administrator registration	Normal
4	Administrator login	Normal
5	Item management	Normal
6	Communication parameter setting	Normal
7	Call the police	Normal
8	Database	Normal
9	Tag reading and writing	Normal

label exceeds 5 meters, its reading rate is extremely low and it has no use value. Of course, in actual usage, the reliability can be increased by increasing the power.

In addition, the effect of different offset angles on the tag read rate was also tested. The results show that the reading rate decreases with the increase of the offset angle.

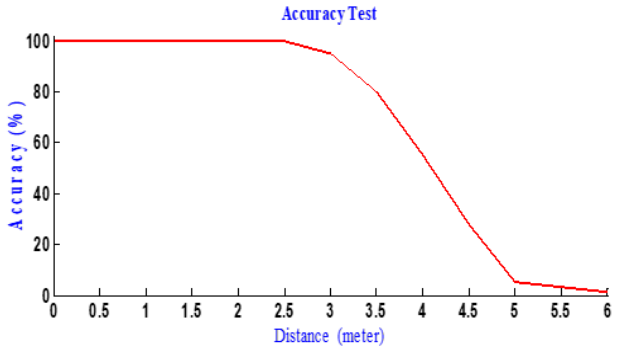


FIGURE 9. Relationship between accuracy and distance.

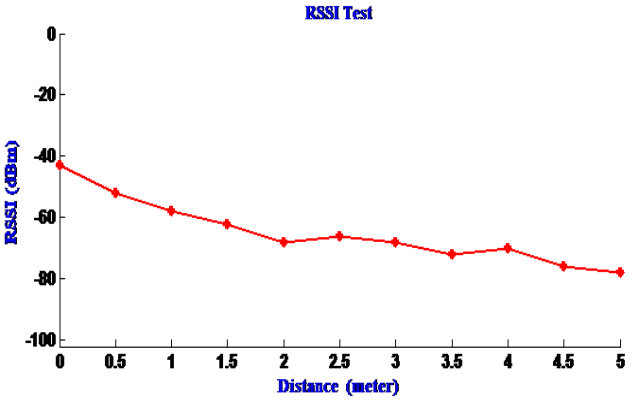


FIGURE 10. Relationship between RSSI and distance.

The effective recognition angle is about 60°, and the effect is better in the range of 45°. After 75°, the reading rate is significantly reduced. Therefore, there is a certain requirement for the position of the cultural relics and the angle of the reader to ensure its reliability.

In a passive radio frequency identification system, Received Signal Strength (RSSI) is the signal strength of a tag's reflected signal. The size of the RSSI has a lot to do with the actual application environment, but it is most closely related to the distance between the electronic tag and the reader and the size of the transmit power. In general, the larger the transmit power, the larger the RSSI; the closer the distance, the larger the RSSI value. In many cases, RSSI is used for ranging and positioning. As shown in Figure 10, the experimental test of the basic relationship between different distances and RSSI in the same environment. Experimental results show that the closer the distance, the larger the RSSI. When the RSSI parameter is above −73dBm, the reader has a high read success rate, good reliability and practical value.

VI. CONCLUSION

The designed scheme of the system meets the expected requirements, and the museum anti-theft system based on the IoT technology is achieved. Through the electronic tag anti-collision technology, the recognition rate of RFID in this system has been greatly improved. In the system, museum staffs can view the state of the museum anytime or anywhere, and it is more effective in regulating cultural relics. The effective

use of RFID identification range is more valuable than the RFID system set at the import and export location, and the anti-theft response is faster and safer. Anti-theft, more concealed than traditional infrared methods, not easy to be invaded. Of course, the museum with anti-theft system based on the IoT can be widely used in other fields, and it has a wide range of market applications and social needs.

Of course, the system has achieved the expected goals, but with the continuous improvement and development of RFID technology, more research and analysis are needed in the following aspects.

(1) The detection accuracy of the hardware part of the system can be further improved to improve the safety of museum equipment.

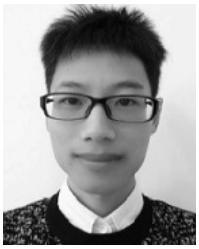
(2) The RFID system has a limited recognition range, which helps to protect the stolen cultural objects and respond to the alarms in time. But for the entire museum, it need more this equipment, resulting in an increment in overall energy consumption, power consumption, and layout.

(3) If there is a certain volume of obstacle between the reader and the tag, it will affect the signal strength, thus affect the packet loss rate. The size of the packet loss rate is closely related to the material, volume and degree of obstruction of the obstacle. In actual applications, adjustment tests should be performed according to actual conditions to ensure the reliability of the system application.

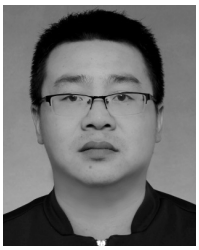
REFERENCES

[1] *One Billion People Visit Chinese Museums in 2018*. Accessed: Jan. 9, 2019. [Online]. Available: http://en.people.cn/n3/2019/0109/c90000-9536237.html
[2] G. Ke and Q. Jiang, "Application of Internet of Things technology in the construction of wisdom museum," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 10, p. e4680, May 2019.
[3] N.-A. Çayirezmez, H.-M. Aygün, and L. Boz, "Suggestion of RFID technology for tracking museum objects in Turkey," in *Proc. Digital Heritage Int. Congr.*, Marseille, France, Oct./Nov. 2013, pp. 315–318.
[4] R. Tesoriero, J.-A. Gallud, M. Lozano, and V. M. R. Penichet, "A location-aware system using RFID and mobile devices for art museums," in *Proc. 4th Int. Conf. Autonomic Auton. Syst. (ICAS)*, Gosier, Guadeloupe, Mar. 2008, pp. 76–81.
[5] J. Landt and C. Barbar, "Shrouds of time: The history of RFID," AIM inc., 2001.
[6] K.-Q. Yan, S.-C. Wang, W.-S. Xiong, K.-Y. Lu, and Y.-J. Cha, "Customer management and marketing strategy development in the Internet of Things," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Sendai, Japan, Nov. 2018, pp. 297–304.
[7] S. B. A. Hamid, A.-D. Rosli, W. Ismail, and A. Z. Rosli, "Design and implementation of RFID-based anti-theft system," in *Proc. IEEE Int. Conf. Control Syst., Comput. Eng. (ICCSCE)*, Penang, Malaysia, Nov. 2012, pp. 452–457.
[8] G. Jayendra, S. Kumarawadu, and L. Meegahapola, "RFID-based anti-theft auto security system with an immobilizer," in *Proc. Int. Conf. Ind. Inf. Syst.*, Penadeniya, Russia, Aug. 2007, pp. 441–446.
[9] Y.-M. Tang, "Research on laboratory management early warning system of Zhangzhou vocational and technical college based on Internet of Things technology," M.S. thesis, School Comput. Sci. Technol., Jilin Univ., Changchun, China, 2015.
[10] Y.-Q. Chen, "Application of embedded RFID in modern interactive museum," M.S. thesis, School Manage., Wuhan Univ. Sci. Technol., Wuhan, China, 2011.
[11] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 161–175, Aug. 2018.
[12] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, Dec. 2018.
[13] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, Apr. 2018, Art. no. 9675050.
[14] M. Ge, H. Bangui, and B. Buhnova, "Big data for Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 87, pp. 601–614, Oct. 2018.
[15] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 1–27, Feb. 2018.
[16] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.
[17] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018.
[18] V. Lakafosis, A. Rida, R. Vyas, L. Yang, S. Nikolaou, and M. M. Tentzeris, "Progress towards the first wireless sensor networks consisting of inkjet-printed, paper-based RFID-enabled sensor tags," *Proc. IEEE*, vol. 98, no. 9, pp. 1601–1609, Sep. 2010.
[19] Z. Meng and J. Lu, "A rule-based service customization strategy for smart home context-aware automation," *IEEE Trans. Mobile Comput.*, vol. 15, no. 3, pp. 558–571, Mar. 2016.
[20] Z. Meng and Z. Li, "RFID tag as a sensor—A reviewon the innovative designs and applications," *Meas. Sci. Rev.*, vol. 16, no. 6, pp. 305–315, Dec. 2016.
[21] Y. Ma, B. Wang, S. Pei, Y. Zhang, S. Zhang, and J. Yu, "An indoor localization method based on AOA and PDOA using virtual stations in multipath and NLOS environments for passive UHF RFID," *IEEE Access*, vol. 6, no. 6, pp. 31772–31782, May 2018.
[22] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, "Taxonomy and challenges of the integration of RFID and wireless sensor networks," *IEEE Netw.*, vol. 22, no. 6, pp. 26–35, Nov. 2008.
[23] A. P. Sample, J. Braun, A. Parks, and J. R. Smith, "Photovoltaic enhanced UHF RFID tag antennas for dual purpose energy harvesting," in *Proc. IEEE Int. Conf. RFID*, Orlando, FL, USA, Apr. 2011, pp. 146–153.
[24] D. De Donno, L. Catarinucci, and L. Tarricone, "RAMSES: RFID augmented module for smart environmental sensing," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 7, pp. 1701–1708, Jul. 2014.
[25] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, and M. M. Tentzeris, "Ambient RF energy-harvesting technologies for self-sustainable standalone wireless sensor platforms," *Proc. IEEE*, vol. 102, no. 11, pp. 1649–1666, Nov. 2014.
[26] M. Akgün, A. O. Bayrak, and M. U. Çağlayan, "Attacks and improvements to chaotic map-based RFID authentication protocol," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 4028–4040, Dec. 2015.
[27] R. Colella, L. Tarricone, and L. Catarinucci, "SPARTACUS: Self-powered augmented RFID tag for autonomous computing and ubiquitous sensing," *IEEE Trans. Antennas Propag.*, vol. 63, no. 5, pp. 2272–2281, May 2015.
[28] X. Liu, B. Xiao, K. Li, A. X. Liu, J. Wu, X. Xie, and H. Qi, "RFID estimation with blocker tags," *IEEE/ACM Trans. Netw.*, vol. 25, no. 1, pp. 224–237, Feb. 2017.
[29] E. Valero, A. Adán, and C. Cerrada, "Evolution of RFID applications in construction: A literature review," *Sensors*, vol. 15, no. 7, pp. 15988–16008, Jul. 2015.
[30] X. B. Yang, "On the anti-theft technology of modern museums," *Mod. Phys.*, vol. 23, no. 5, pp. 43–46, Oct. 2011.
[31] Y. C. Shen and S. Q. Shen, "Radio frequency identification technology and its development status," *Electron. Technol. Appl.*, vol. 1, pp. 2–3, Jan. 1999.
[32] W. Xiaohua, "Research on anti-theft problem in RFID library," *China Electron. Commerce (RFID Technol. Appl.)*, vol. 4, no. 3, pp. 35–37, Jun. 2009.
[33] K. Michael and L. McCathie, "The pros and cons of RFID in supply chain management," in *Proc. Int. Conf. Mobile Bus. (ICMB)*, Sydney, NSW, Australia, Jul. 2005, pp. 623–629.
[34] F. Sahba, "Museum automation with RFID," in *Proc. World Automat. Congr. (WAC)*, Waikoloa, HI, USA, Aug. 2014, pp. 19–22.
[35] J. Shi, "Innovative application of long-distance RFID in security field," *China Public Saf. (Comprehensive Ed.)*, vol. 5, pp. 71–74, May 2006.
[36] Z. G. Feng, "Analysis of the theory of wisdom museum," *Museum Res.*, vol. 1, pp. 19–25, Feb. 2019.
[37] X. Y. Du, "Discussion on the application of Internet of Things technology in the construction of digital museums," *Cultural Relics Appraisal Appreciation*, vol. 15, pp. 130–131, Aug. 2018.

ZELIANG LIU was born in 1980. He received the B.S. degree from Central China Normal University, Wuhan, China, in 2003, and the M.S. degree from the Wuhan University of Technology, Wuhan, China, in 2009. He is currently an Associate Professor with the School of Electronic Engineering, Jiujiang University, China, and a Visiting Scholar with Wuhan University. His research interests include wireless sensor networks, the Internet of Things, and communication and information systems.



MIN WANG received the B.Sc. and M.Sc. degrees from Yunnan University, Yunnan, China, in 2015 and 2018, respectively. He is currently pursuing the Ph.D. degree in computer science from Wuhan University, Wuhan, China. His research interests include in the areas of deep learning and vehicular ad hoc networks.



SHIKAI QI was born in Qianjiang, Hubei, China, in 1987. He received the B.S. and M.S. degrees in physical electronics from the School of Physics and Electronic Engineering, Henan Normal University, in 2013, and the Ph.D. degree in physical electronics from the Chinese Academy of Sciences University, Institute of Electronics, Chinese Academy of Sciences, in 2016.

From 2016 to 2019, he was an Associate Professor with the School of Electronic Engineering, Jiujiang University, Jiangxi, China. His research interests include application of high-power microwave devices in military and production, vacuum electronics, hot and cold cathode, and application of photocathode in high power microwave devices.

CHANGCHUN YANG was born in Anhui, China, in 1979. He received the B.S. degree from the College of Physics, Anhui University, in 2002, and the Ph.D. degree in nuclear science and engineering from the Chinese Academy of Sciences (CAS).

From 2005 to 2010, he was a Doctoral with CAS. He was a Doctoral, an Associate Professor, and an Associate Dean. Since 2011, he has been involved in research on nondestructive testing. He is currently with the College of Electric Engineering, Jiujiang University. His research interests include superconducting technology and insulation technology.