Research and Implementation of Implantable Medical Device Authentication

To cite this article: Wenwen Yang and Fan Zhang 2018 J. Phys.: Conf. Ser. 1069 012152

View the article online for updates and enhancements.

Related content
- Advanced Secure Optical Image Processing for Communications: Single-pixel optical information encoding and authentication
  A Al Falou
- Multiparty Simultaneous Quantum Identity Authentication Based on Entanglement Swapping
  Wang Jian, Zhang Quan and Tang Chao-Jing
- Multi-Style Migration QR Code
  Fucheng You, Shuren Lai, Hechen Gong et al.
Research and Implementation of Implantable Medical Device Authentication

Wenwen Yang and Fan Zhang
College of Information Science and Technology, Agricultural University of Hebei, No. 298, Lingyusi Street, Nanshi District, Baoding City, Hebei Province, China
Email: 15231230810@163.com

Abstract. In order to solve the problem that the implantable medical device has not realized the certification test, this paper designs the main process of authentication detection. After the patient was implanted the medical device, the hospital acquires the patient's image and other basic information through the camera, stores it in the implantable medical device authentication system, and generates a paper version and an electronic version certificate; After the patient is discharged from hospital, the hospital issues and informs the patient to obtain the certificate; When patients come in and go out the important places or need security check, they can show their certificates, and the authentication person will automatically jump to the implantable medical device authentication system by using the QR code in the APP scanning certificate, and obtain the image address by Key in Map, find and restore the patient image from the system database. Finally, the patient image generated after the decoding of QR code is matched by SURF algorithm and PAOSAC algorithm, if the match successfully represents the legal and safety of medical devices implanted in patients. If the match fails, the authentication person can verify the legal security of the implanted medical device through the data examination and comparison. At this point, complete the certification testing of implantable medical device.

1. Introduction
With the development of information technology, people are paying more and more attention to the safety issues of medical devices. The safety traceability issue of implantable medical devices is a core element of medical safety and an important target for hospital risk management. Based on this understanding, this paper aims to strengthen the safety of using implantable medical devices, proposes a method for the certification of implantable medical devices, and studies the implementation of this method. Due to the high error rate of human eye recognition and the feasibility of the existing RFID technology to achieve the matching is low. So, this research use the face image matching algorithm is used to achieve the authentication and detection.

After the implantable medical device is implanted in the patient's body, the certification test of the medical device is not involved. This brings inconvenience to the travel of the implanted medical device user and increases the risk of medical device management. The implanted medical device certification test is to solve the problem that the authentication person identifies the implanted medical device when the patient has been implanted with the medical device, and simplifies the certification process and saves time. It is also a guarantee of patient safety. After the patient implants the medical device, the hospital generates a paper version and an electronic version of the certificate, and stores the patient's basic information in the database of the implantable medical device authentication system. On the one hand, the image of the patient was reduced to the patient image by scanning the QR code and preprocessed into a comparable face image A. On the other hand, by calling the system interface
to obtain the patient image in the database and preprocessing it into a comparable face image B. The image A and the image B complete the matching of the face image. If the matching between the images A and B is successful, it proves to be the person. Otherwise, the authentication person need to confirm again and judge the validity of the information.

2. System Design

2.1. B/S Mode Based on Authentication System

There are many kinds of implantable medical devices and its materials are complex, establish an authentication system based on B/S mode, it solves the problem of low portability and poor scalability of traditional C/S mode. This system used the back-end database for its core and it is convenient for connecting clients and hospitals, and it can achieve data sharing and information sharing. So, the computational efficiency of the application is improved. The system is implemented through a full-stack lightweight open source framework. Its development advantages include convenient decoupling, simplified development, and better service support.

The users of the authentication system are mainly hospitals and authentication person: The hospital enters the basic information of the inpatient into the system database and the patient receives the certificate with the QR code after leaving the hospital. When the authentication person conducts authentication, the system information database is acquired by scanning the QR code jump authentication system to obtain the patient information. Figure 1 shows the authentication system UML.

![Figure 1. The authentication system UML.](image)

2.2. Design the APP Scan Code

QR Code (Quick Response Code) is a matrix 2D barcode developed by Japan. The APP scan code is corresponding the decoding of the QR code. The successful decoding of the QR code means that the authentication system data has established the correct connection. It is related to whether the authentication person can use the APP and the authentication system data to perform certification testing, and is also directly related to the legitimate rights and interests of patients implanted with medical devices. The image acquisition of the QR code is to design and implement APP scan code and use the phone's own camera. The APP directly calls the class of camera, Android. Hardware. Camera, to shoot, and when this class is being used, it is needed to declare the Camera permission in Android.

In order to enable the authentication person to obtain information, the authentication person’s
mobile phone must download scan code APP. The QR code is identified by using the APP to scan the QR code. The authentication person registers the personal account of the certification. After the registration is successful, they enter the APP for authentication.

2.3. Face Image Matching
The patient's face image obtained from the QR code after scanning the APP, and the face image of the patient in the database of the authentication system is called to perform face image matching. The premise of the mobile phone APP acquiring information is that the client loads the authentication system, and scan QR code by APP. So, actively associate with the authentication system database. Have a direct access to QR code information and implantation of medical device patient information. At the end, APP shows the information.

When the authentication person conducted a scan code authentication through the APP, associated with the certification system, and compared with the patient image from the authentication system, if the comparison is successful, the APP returns to the successful interface; if failed, it will suggest authentication person to recognize by human eyes. If the authentication person's eyes are successful, the information can be submitted in the authentication system and updating the system library.

Face image matching is a branch of image matching. Due to the distribution of facial features, face image matching can be divided into four parts: pre-process the face images; face detection; feature point extraction of face images; Face image matching. Figure 2 shows the general flow of face image matching.

2.4. Database Design
This database design includes the authentication system database and the APP scan code database. The included tables mainly cover the basic information of patients, hospitals and doctors, medical devices and authentication person, authentication test information, and two-dimensional code information. The creation of the above data table follows the principle that a table corresponds to the information of an entity or object. Each data table cooperates with each other to jointly achieve medical device certification testing. The name of the main database table is shown in Table 1.

| Name                        | Table Name     |
|-----------------------------|----------------|
| Patient information sheet   | Patient_info   |
| Hospital information sheet  | Hospital_info  |
| Doctor's information sheet  | Doctor_info    |
| Authentication person info  | Test_Person_info|
| Authentication test data    | Authenticate_info|
| Paper certificate info      | Paper_info     |
| Electronic certificate info | Electronic_info|

Figure 2. The general flow of face image matching
3. System Structure and Function Implementation

3.1. System Module Division
The purpose of designing the system is to achieve implanted medical device certification test. The implementation of authentication test is mainly divided into three modules: authentication system, APP scan code and face image matching. The system functions are divided into APP and server. APP-side function: scanning QR code - QR code information display-authentication test information display. Server-side features: QR code generation - input the database information - modify the database information - maintain the information.

3.2. The Function of Each Module

3.2.1. Authentication System. The main interface of the authentication system is divided into six modules: patient information, QR code interface, APP interface, basic information, certification information and development tools.

- **Patient information.** The hospital can generate the patient's corresponding hospital information, personal information, nursing information and medical records by querying the patient ID, also can directly add new patient information. The import and export function can facilitate hospital management. The patient or family can fill in the information by hand and the hospital automatically stores it in the system database.

- **Basic information.** The basic information is to management and query the hospital information. The doctor can query the corresponding information through the hospital ID, including the hospital's location, hospital's distribution, the medical team, surgical records, patient records, hospital departments, operation details, communication and discussion, and successful cases, problem solving, paper certificates, electronic certificates and other information. Doctors can add basic information directly in the page, and the import and export function allows doctors to upload and download hospital information and achieve unified management.

- **Certification information.** The Certificate information is to generate patient's paper certificate and send electronic certificate. The doctor enters the patient ID and automatically calls the database to generate the patient's name, operating time, patient photos and other related information. Eventually generate the authentication test QR code.

- **QR code generation.** QR code generation uses the base64 encoding to generate a string concatenated to the authentication system's URL and then to embed the QR code. When the APP scans the code, the corresponding URL page is automatically opened, and decode the parameters into a picture by decoding, and call the system interface, find the patient's images in the system through the KEY. In the end, through face image matching to achieve authentication test. Figure 3 shows the QR code decoding flow chart.

3.2.2. APP Authentication. The APP scan code is mainly used to decode the information that contained in the QR code, and to obtain the required information when scanning the code. And match
the corresponding information in the authentication system database for face image matching.

The QR code mainly contained the authentication URL and the basic information of the implanted medical device patient. As a lightweight database, the SQLite database satisfies the user's need for database information browsing. After scan the code, we get the result information of the face image matching. Finally, the system matches the face image and returns the result to the APP.

3.2.3. Face Image Matching. This paper uses SURF algorithm and PROSAC algorithm to achieve face image matching. Traditional human eye recognition has a large workload and a high error rate. With the development of information technology, scan code matching through RFID technology has also been applied. However, RFID technology requires certain hardware support, low feasibility, and poor security. The image matching through the algorithm not only reduces the artificial labor force, but also has a high accuracy, and it also guarantees the safety of patient information.

SURF algorithm is more robust and faster than SIFT algorithm. As Bay said, the SURF algorithm's speed is at least three times faster than the SIFT algorithm, and the synthesis is higher than the SIFT algorithm [8]. The SURF algorithm has these advantages because the algorithm is properly simplified on the basis of the SIFT algorithm, and the integral image is used multiple times to improve the algorithm speed. The core of SURF algorithm is Hessian matrix. The Hessian matrix marks the image's feature points with extreme points, and reduce image matching time by integrating images.

The PROSAC algorithm has a mismatching problem in the feature pre-matching results of SURF algorithm. According to the matching degree of feature matching point pair, the similarity degree sample is taken as the interior point of the model. The model is determined according to the data, and the number of internal points is proportional to the model's reference rate. Assuming that a, a′ is a pair of correct matching point pairs in the matching image, then the limit constraint of the a, a′ basic matrix representation is:

\[ aF_{a}a' = 0 \]  

Where F is the fundamental matrix.

The PROSAC algorithm samples and obtains the basic subset from the matching results, and according to the basic subset to estimate the fundamental matrix F. Finally, the erroneous matching point pair is eliminated through the base matrix F. The speed of the algorithm generally starts with two aspects: one is to reduce the time required for model parameter testing, and the other is to reduce the number of samples. If the algorithm is reduced, the confidence of the algorithm will be reduced. So, this paper combines the advantages of PROSAC algorithm to improve the speed of the algorithm by reducing the time required for model parameter verification. This ensures that the confidence of the algorithm remains unchanged. Moreover, reducing the time required for the model parameter test only needs to reduce the number of algorithm model parameters and ensure that the total data amount does not change. This can ensure the validity of the algorithm.

4. Conclusion
The management of medical devices involves all aspects of people's lives. Through the research of face image matching technology for implanted medical device certification testing, this not only improves the management efficiency and safety, but also protects the legitimate rights and the interests of patients. This paper combined the PROSAC algorithm and based on the traditional SURF algorithm to achieve face image matching. This improved the image matching accuracy and the matching time. The APP scan code is realized by using the mobile phone's own resources, and use the QR code itself to read and respond to the characteristics of the medical device.

Authentication detection. This can effectively and conveniently realize the scan code. However, due to lack of experience, there are still many areas for improvement. For specific applications, it is very important to reduce the complexity and computational complexity of the algorithm. And how to achieve certification testing more quickly and more accurately is an important problem that needs further study.
5. Reference

[1] WEI Wei, MA Junfu. Self-Adaptive Fast Face Color Transfer [J]. Journal of Image and Graphics, 2016, (02): 129-134.

[2] Wang Yang. Design and implementation of medical device warehouse management system based on C/S mode [D]. University of Electronic Science and Technology, 2014.

[3] Gao J Z, Prakash L, agatesan R. Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution [C] // Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International. IEEE, 2007, 2: 49-56.

[4] Liu Yanmei, Song Yitao, Dong Lei. Cross-platform heterogeneous database system based on B/S structure [J]. Computer System Application, 1998, (08): 9-10 + 23.

[5] Ma Ming, Li Haibo. Design and implementation of two-dimensional code generation and recognition system based on Android [J]. Computer Knowledge and Technology, 2012, (26): 6353-6356.

[6] Liu Haiyang, Li Chunming, Wang Mengmeng, Xuan Zongze, Yang Pengfei. Image adaptive matching based on SURF and improved RANSAC algorithm [J]. Machinery and Electronics, 2017, 35(03): 73-76.

[7] Zhang Xueqin, Liu Yuanyuan, Cao Yichen, Zhang Pengfei. A cloth image matching algorithm based on improved SURF and K-Means clustering [J]. Journal of East China University of Science and Technology, 2017, 43(01): 105-112.

[8] H. Bay, A. Ess, T. Tuytelaars, L. V. Gool. Speeded-Up Robust Features (SURF)[J]. Computer Vision and Image Understanding. 2008, 110(3): 346 - 359.

[9] Sharma P, Sharma S, Scholar P G, et al. Face recognition and detection using hausdorff distance, SURF and SVM [J]. International Journal of Engineering Science, 2016: 3112-3114.

[10] Ran Juanhong. Research on block weighted face recognition system based on SIFT [D]. Chang’an University, 2015.