TELKOMNIKA, Vol. 11, No. 9, September 2013, pp. 5284~5292
ISSN: 2302-4046

The Research of Mobile Phone Entrance Guard System Model Based on the Encryption Two-dimensional Code

Chu Jianli*[a], Sun Yongdao[b], Liu Xia[c]
Department of Information Engineering, Xingtai Polytechnic College, Xingtai, Hebei Province, China,
Ph: 13323195999[a], 13831981090[b], 8633694703[c]
*Corresponding author, e-mail: xpcchujl@126.com, 283281266@qq.com

Abstract

This article designs a new mobile-phone entrance guard system, uses the encryption two-dimensional code for identity authentication. Different from other similar products in the market, this system does not rely on specialized mobile phone card or NFC (near field communication) module. It can be directly realized through mobile-phone software, and it can be operated simple and safer. This article designs the whole system model, includes structure, function and workflow. It also analyzes and researches the main algorithms used in the system, which include security policy algorithm, encryption two-dimensional code algorithm and image recognition algorithm. Finally, it provides the solution method for the problem in the experimental simulation. It also evaluated and summarized the experimental results.

Keywords: *mobile-phone entrance guard system, encryption two-dimensional code, security policy, image recognition algorithm*

1. Introduction

The development of the intelligent mobile-phone technology is so fast in recent years. Because many key technologies have been breaked through, the function of mobile-phone has been changed from the traditional call to the integrated application terminal [1-2]. This article mainly studies the intelligent mobile-phone application in entrance guard field. The intelligent mobile-phone can be used to instead of traditional card and keys. Now, most of the mobile-phone entrance guard system in the market use special mobile-phone card or NFC (Near Field Communication) module to communicate with card reader equipment in the system. And obviously, this is not suitable for mass users. The system this article provides does not rely on any special hardware, can directly realizes identity authentication by mobile-phone software, and realize more management functions.

There are many ways to realize entrance guard identity authentication by mobile-phone software. After comparison, this article chooses the encryption two-dimensional code to realize identity authentication. This method has the advantages of low cost and simple operation process. Also, it can be safer.

According to certain rules of the plane(in two-dimensional direction), the two-dimensional code [3-6] uses some specified geometrical figure to distribute black and white graphics to record data symbol information. This technology has been widely used in the field of find by hard and thorough search and data entry. But the two-dimensional code as the electronic key for identity authentication is also a kind of innovative applications. The two-dimensional code has so many kinds. After comparison, finally this article chooses QR code. Because it can contain large capacity information, be high reliability, low cost, and can express the single-byte, multibyte (as Chinese character) and image information and so on. It also has strong confidentiality and security. The most important is the speed for encoding and decoding of QR code is fast, which is very suitable for the requirements of the entrance guard system to the reaction speed.

2. System Model Design Method

The system consists of mobile-phone client software, entrance guard terminal equipment and system server (as shown in Figure 1).

Received February 17, 2013; Revised June 10, 2013; Accepted June 21, 2013

(1) The function of mobile-phone client software is to generate or get the encrypted two-dimensional code image to realize identity authentication. This system combines the two architectures of B/S and C/S, so people can use more mobile-phone with different brands. Android phone or iPhone can directly install the client software. Other phones can get the encryption two-dimensional code image dynamically from the server.

(2) The function of the entrance guard terminal equipment is to identify and decrypt the two-dimensional code images, and to decide whether to open the door. It consists of the controller、the special power supply and electromagnetic lock. The controller consists of core board based on S3C6410 processor, LCD display screen, camera, proximity switches and electric relay.

(3) The function of the server is to manage all rooms, all users and user privileges. One room can be operated by multiple users. One user also can operate multiple rooms (as shown in Figure 2).

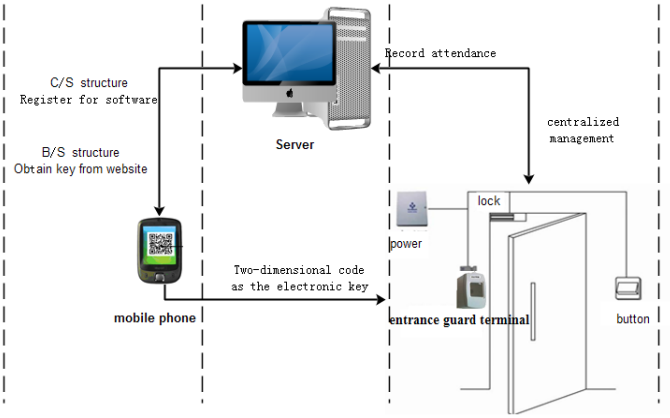


Figure 1. The whole System Model

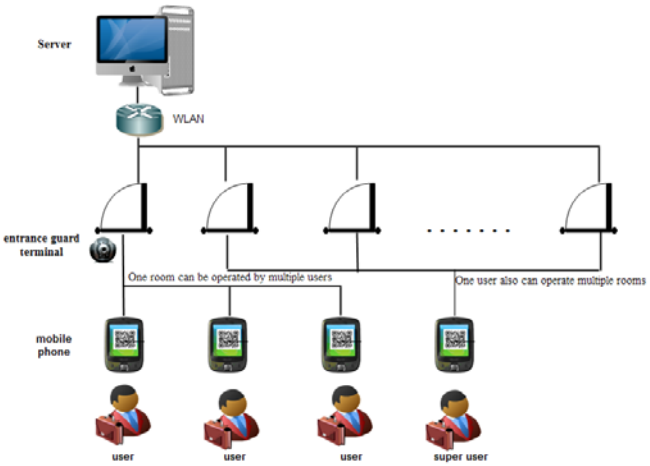


Figure 2. Multiple-Rooms and Multiple-Users Management Model

The system's workflow is like this: The user starts mobile-phone software and generates the encryption two-dimensional code image. Then put the mobile-phone on the slot of the entrance guard terminal equipment. It will trigger the proximity switches in the slot, and then the whole image recognition process will be started. If the recognition result is correct, it proves that this is a legitimate user, the door will be open. If not correct, the door will not open, at the same time, the LCD display screen will show the failure reason information.

3. Research Method

3.1. The Security Strategy

To ensure the security of this system, we formulate a series of effective security strategies, which include password protection for mobile-phone software, enciphered message and user rights management and so on. Those security strategies can protect the legal users, and at the same time refuse the illegal users to use and counterfeit. But it still has a problem: the image can be copied easily. So how to prevent others from malicious copy and steal? To resolve this problem, this article makes two security strategies to protect image's safety.

(1) Two-dimensional code image will be expired if timeout: The generated two-dimensional code image must be used immediately. Otherwise, it will be expired if timeout.

(2) Two-dimensional code image only can be used once: The image must be used only once. It will become invalid at the second times.

The core algorithm to realize the safety strategies above are adding the time-stamp into the two-dimensional code for determines the effectiveness of the image. The entrance guard terminal equipment needs to proofread the time-stamp. If it's timeout, the two-dimensional code is set to expire. At the same time, the terminal equipment records the time-stamp which used at the current effective time, to ensure it must be used only once. It will become invalid at the second times. So even legitimate two-dimensional code image is stolen or copied by other people, they must use it at a very short time. But at the very short time, the legal users maybe already used it. Other people can't use it again. So it's good for protecting the safety of the two-dimensional code image. The complete judgment process for the two-dimensional code image is shown in Figure 3.

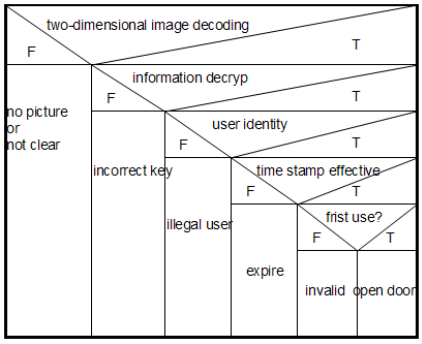


Figure 3. The N-S diagram of judgment process for the two-dimensional code image

3.2. Encryption Two-dimensional Code Algorithm

In the system, the core algorithm of mobile-phone client software is the encryption two-dimensional code algorithm [7], which includes identity authentication information collection, information encryption, Base64 encoding and QR code encoding. The whole algorithm process is shown, as shown in Figure 4. The following will detail each algorithm design.

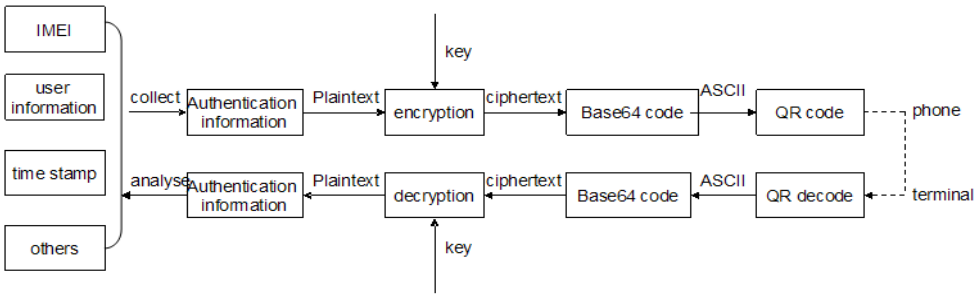


Figure 4. Encryption Two-dimensional Code Algorithm Process

(1) Authentication Information Collection

At first, mobile-phone client software must collect the information for authentication. This needs to consider the functional requirements of the system. After analysis, the authentication information for identifying should include the mobile-phone IMEI (International Mobile Equipment Identity) number. IMEI is the 15 digits “electronic serial number “which is the world's only mobile-phone identifier. The authentication information also includes the basic user information, such as name and job. This information can be displayed in the LCD screen in the entrance guard terminal equipment. Finally, the authentication information should include the time-stamp to determine the valid of two-dimensional code image, as shown in Figure 4.

(2) DES Encryption

The authentication information must be encrypted. Otherwise it can easily be cracked and imitation. According to the difference of the cipher keys, it can be divided into symmetric encryption and asymmetric encryption [8-12]. Symmetric encryption is represented by DES algorithm. Asymmetric encryption is represented by RSA algorithm. Considering we will make the mixed use of cipher text and QR code, we need to ensure the decoding speed. Finally, we select DES algorithm, because it can be decoded quickly. At the same time, the DES algorithm has high security. Even other person uses exhaustion method to attack, it also impossible to be cracked. DES encryption steps are shown as Figure 5.

Step 1: Computing cipher keys. The user input a 64 bits cipher keys. Take away the 8 bits check code. The remaining 56 bits are the effective cipher keys. After substituting, grouping, shifting and iterative processing the 56 bits key, finally it obtains 16(K_1 -K_{16}) sets of son key.

Step 2: Plaintext is grouped and substituted. The plaintext is grouped of 64 bits, and is substituted according to certain rules. After that, it’s divided into the two groups which are the left (L_0) and the right (R_0), and each group has 32 bits.

Step 3: Iterated operation. It needs iterated operation 16 times. Each iteration formula is as follows, where “i” means the number of iterations, “⊕” means every bits modular 2 and summation.

$$L_i=R_i\text{-}1 \qquad i=1, 2, 3...16 \tag{1}$$

$$R_i=L_i\text{-}1 \square f\ (R_{i-1}, K_i) \quad i=1, 2, 3...16 \tag{2}$$

Step 4: Getting cipher text. The $R_{16}L_{16}$ got from step3, are reverse substituted to get the cipher text.

The DES encryption algorithm is opposite the decryption algorithm. That will not be described in detail here.

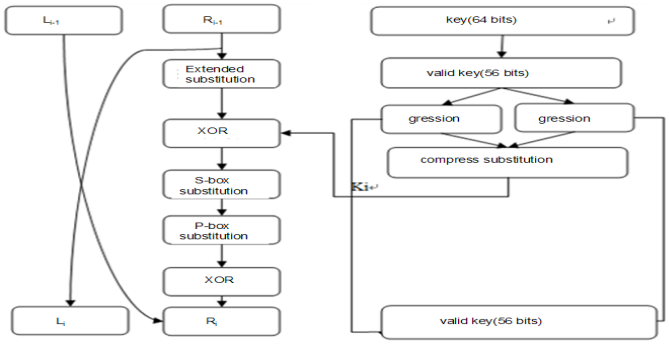
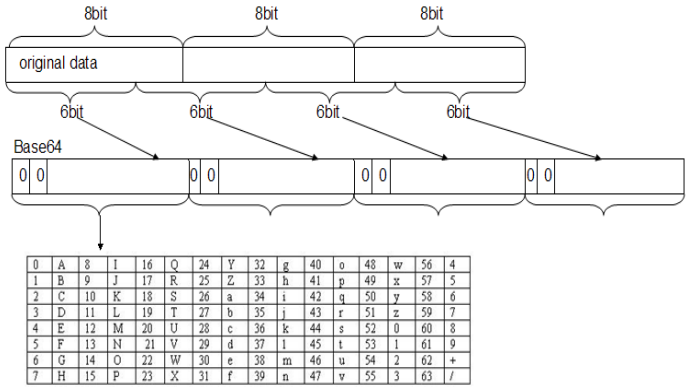


Figure 5. DES Encryption Algorithm Description Graph

(3) Base64 Encode Conversion

The encrypted data cannot be displayed. The reason is the original data which was encrypted by DES algorithm has been completely different, some have even exceed the range of the character table. Therefore, the cipher text cannot be directly converted to QR code. In order to solve this problem, it needs Base64 encode conversion. Before QR encoding, the cipher text will be split and recombined, and become a new string which can be displayed.

The principle [10-11] of Base64 encode conversion is: the 3 bytes of 8 bits (3*8=24) is converted into 4 bytes of 6 bits (4*6=24). After that, at the head of every byte of 6 bits adds two zero, formed to every byte of 8 bits. Each byte value is replaced by the character of the coding table in Figure 6. The characters of this coding table consist of the English characters, figures and common symbols. Even if the original data byte value exceeds the boundary value, it finally returns to the range of ASCII table because of split and recombine.



0	A	8	I	16	Q	24	Y	32	g	40	o	48	w	56	4
1	B	9	J	17	R	25	Z	33	h	41	p	49	x	57	5
2	C	10	K	18	S	26	a	34	i	42	q	50	y	58	6
3	D	11	L	19	T	27	b	35	j	43	r	51	z	59	7
4	E	12	M	20	U	28	c	36	k	44	s	52	0	60	8
5	F	13	N	21	V	29	d	37	l	45	t	53	1	61	9
6	G	14	O	22	W	30	e	38	m	46	u	54	2	62	+
7	H	15	P	23	X	31	f	39	n	47	v	55	3	63	/

Figure 6. Base64 Encode Conversion Algorithm

(4) QR Encoding Algorithm

After Base64 encode conversion, the information consists of English characters, numbers and common symbols. It can be directly converted into QR code. The process of QR code encoding has 7 steps [12], includes the data analysis, data encoding, error correction encoding, constructing the final information, layout module in a matrix, masking, adding format and version information. Because the QR code of this system needs to handle only letters and numbers, so the data encoding uses alphanumeric mode (mode indicator code is 0010). The inputted characters ($C_1C_2...C_n$) will be converted into the numerical ($D_1D_2...D_n$) according to the specific coding table. Every two digits are as a group. According to the formula, it will be converted to binary sequence ($B_1B_2...B_{n/2}$). Finally, at the head of the binary sequence above adds the mode indicator code and the characters' count indicator code. Then the process of data encoding completes. The formula is as follows.

Step 1: $C_1C_2...C_n$ ==>$D_1D_2...D_n$ ==> (D_1, D_2), (D_3, D_4)..... (D_{n-1}, D_n)

Step 2: B1=f (D_1, D_2) = $(D_1*45+D_2)_2$

Step 3: (Mode indicator $0010)_2$+ (characters' count indicator) $_2$+ ($B_1B_2...B_{n/2}$)

According to the different versions and error correction levels, QR encoding will have little different . It's will not described in detail here.

3.3. The Image Recognition Algorithm

QR code image recognition [13-19] is implemented in entrance guard terminal equipment. The main problems of QR code images which are collected by the camera include incline、distortion and illumination unevenness. Therefore, before QR decoding, we first need to solve these problems. The algorithm will directly influence the system's identification efficiency and reaction speed. The main steps are as follows.

(1) Reducing Image Memory Spending

The camera photographs are mostly color images. Color image with large amount of data is not convenient for subsequent processing. So first of all, it must reduce the image memory spending. Color image needs to be converted to gray image. In the past, a pixel is represented by three RGB color components, now is represented by one gray value. The image memory spending is reduced of 2/3. Gray image transform standard formula is:

$$W=0.30R+0.59G+0.11B \quad (3)$$

R/G/B is the color component value. Gray image is as shown in Figure 7.

(2) Remove Image Noise

The images collected by the camera will produce a variety noise, influence the image recognition effect. So the image has to be removed the noise before recognition. After analysis, the image noise is produced mainly by the optical collection system. This noise accords with the salt noise with Poisson distribution. Median filtering which using the appropriate size of the square window can remove the salt noise [13-14]. This is very suitable for QR image, as shown in Figure 7.

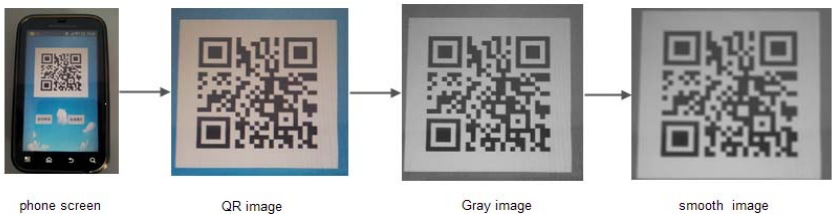


Figure 7. Gray processing and Median Filtering

(3) Image Rotation and Correction

The QR code image which is collected by the camera usually has a deflection angle. Therefore, before recognition it must be rotated to the horizontal direction. First thing is to detect image's horizontal deflection angle, then we can rotate the image according to the angle. The steps to detect image's horizontal deflection angle include images binary processing, edge extraction and Hough transform. Finally, the image should be counterclockwise rotated according to the angle of deflection.

Step 1: Images binary processing [15-16]. It means the image only has two values, the black (gray value is 0) and the white (gray value is 1). The gray image's values is between 0~255. It needs to select the appropriate threshold to segment to determine the pixels value. The purpose of the binary processing is as much as possible to keep back the original image feature, and give up the redundant information. The key of the algorithm is the selection of threshold value. Because the two-dimensional code image is the rectangular module in black and white, the histogram is very ideal. We can see from the Figure 8, the gray value mainly concentrated in the 180 and 20. So we can select 100 (the average values of 180 and 20) as the image threshold. And it's very suitable for binary processing of QR code image, as shown in Figure 8.

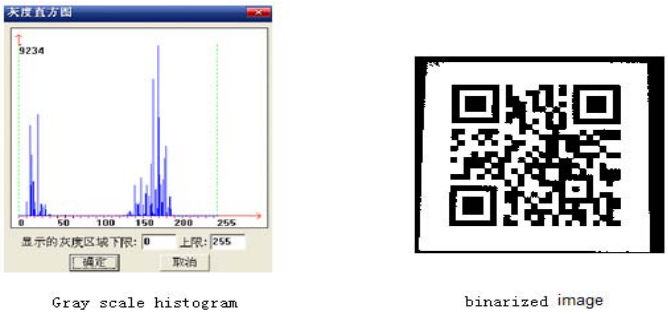


Figure 8. Gray Histogram and the Two Value Image

Step 2: Edge Extraction. It means to detect the edge of the two value image. Here it only needs to detect the horizontal edge. We can use level operator in the Sobel operator to do the faltung process for image. The edge image would be got by threshold processing. The main formula is [15]:

$$E=M \oplus PH > \text{threshold} \quad (4)$$

The results of edge detection are as shown in Figure 9.

Figure 9. Edge Extracting

Step 3: Hough Transform [17-19]. The deflection angle can be obtained through Hough transform. If we know the regional shape in advance, the Hough transform can get the boundary curve very conveniently, and connect the edge dots with discontinuous pixel. The principle of the algorithm is: The linear L in x-y plane can be represented by the formula in Figure 10, where "ρ" means the vertical distance from the origin to the straight line, and "θ" means the angle between the vertical line and X axis.

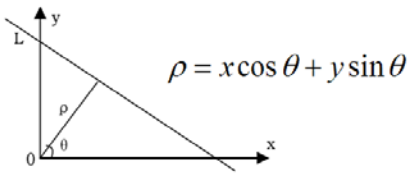


Figure 10.The Parameter Corresponded with a Line on the x-y Plane

The value of "θ" is set of 0o~180o, and the value of "ρ" is set of the image height. Then we create the (θ,ρ) matrix, and select each black pixel in the image to put into the formula above, and calculate value for each θ. The accumulated value of the corresponding value in (Q, P) matrix adds 1. The largest accumulated value is corresponded the QR code image's horizontal line. And the tilt angle corresponding is 90o-θ. Therefore, the image needs to be counterclockwise rotated of 90o-θ.

Step 4: Image rotation and correction [19]. The image rotation formula is as follows, where (x_0, y_0) is the pixel value of original image, and (x_1,y_1) is the pixel value of rotation image.

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \quad (5)$$

The rotated image usually has little distortion. The reason is the new coordinate values are not necessarily as integer. It still needs to use gray level interpolation to calibrate.

After a series of processing, the QR code image can be decoding operation, which is the inverse process of encoding. And that will not be described in detail here.

4. Results and Analysis

The main problem in the experiment simulation is jitter caused by mobile-phone. The original idea is to let the user put mobile-phone screen in front of the camera of the entrance guard

terminal equipment for taking the picture. But we find due to the jitter caused by mobile-phone, the image is not clear and the recognition rate is very low. So we built a confined space. In this space, we created a good environment, suitable for the demands for two-dimensional code image displayed by mobile-phone screen. There is a mobile-phone slot in the entrance guard terminal, which inside has the proximity switch. User put the mobile-phone into the slot to trigger the proximity switch. As a result the whole recognition process is started. The experimental simulation model is as shown in Figure 11.

Figure 11. The Experimental Simulation Model

After repeated experiments, we obtained good experimental effect. First, the recognition rate of this system is high. It's not affected by the size of the mobile-phone appearance. Secondly, reaction speed is fast. The total time of identification and open the door is about 1 second. Finally, the safety performance of this system is high. Even two-dimensional code image was stolen or copied, other people unlikely to be used. If the mobile-phone is lost, user has to immediately notify the server to cancel the user power of this phone. This does not affect the normal use of other users. At the same time, the mobile-phone software has the boot password, even if the mobile-phone is stolen, anyone could not start the software without password.

4. Conclusion

The mobile-phone entrance guard system as a new type of digital entrance guard system, not only can replace the traditional cards and keys, become a comprehensive application of the terminal, but also bring fresh experience for user. It's worth trying as the application and research trend. The system in this article does not rely on special hardware conditions, will be more convenient for promotion and popularization. It can be used in high-grade hotels, office. It also can be combined with the electronic payment, used in public places such as museums, zoo, park and so on. It can promote the use of electronic tickets.

References

[1] Ma Zhenghua, Sun Yuqiang, Shi Hai-feng, Wang Mingfei. The Design of the Embedded Intelligent Safeguard Muti-Identification. *Microcomputer Information*. 2005; 21(12-2): 4-5.
[2] Xiao Quanqin, Liu Mingjun, Liu Yue. Reseach on Mobile 2D Barcode. *Cards World*. 2008; 2(2): 48-50.
[3] Sun Aidong, Sun Yan, Liu Caixing. *The QR-code Reorganization in Illegible Snapshots Taken by Mobile Phones*. Proc. of the 5th International Conference on Computational Science and Applications. Guangzhou, China. 2007: 532-536.
[4] Lingyan Bi, Zewei Fen, Min Liu, Weining Wang. *Design and Implementation of the Airline Luggage Inspection System Base on Link Structure of QR Code*. Electronic Commerce and Security (Conference). China. 2008; 78-83.
[5] Cheng Hongzhou, Liu Xia. *The Research for Mobile Phone Access Control System Based on the Encrypted Type QR-Code.* Science & Technology Vision. 2012; 25: 191.
[6] LIAO Zhao-lai, HUANG Ting-lei, WANG Rui, ZHOU Xiao-yan. *A Method of Image Analysis for QR Code Recognition*. 2010 International Conference on Intelligent Computing and Integrated Systems Conference. Guilin. China. 2010: 250-253.
[7] Qiang Tang. *Public key encryption schemes supporting equality test with authorization of different granularity*. *IJACT(International Journal of Applied Cryptography)*. 2012; 2(4): 304-321

[8] Keita Emura, Atsuko Miyaji, Kazumasa Omote, Akito Nomura, Masakazu Soshi.*A ciphertext-policy attribute-based encryption scheme with constant cipher text length*. IJACT (International Journal of Applied Cryptography).2010; 2(1): 46-59.
[9] Kuo-Ching Liu, Hui-Feng Huang. *A New Design of Encryption/Decryption for Field Applications.* JCIT (Journal of Cases on Information Technology). 2010; 5(5): 39-43.
[10] Jinhui Sun, Geng Zhao, Xufei Li. *An Improved Public Key Encryption Algorithm Based on Chebyshev Polynomials*. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2012; 11(2): 2035-2043
[11] Yong Zhang, Jiali Xia, Peng Cai, Bin Chen. *Plaintext Related Two-level Secret Key Image Encryption Scheme*. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2012; 10(6): 1254-1262
[12] ZHANG Huan-Guo, FENG Xiu-Tao, QIN Zhong-Ping, LIU Yu-Zhen. *Research on Evolutionary Cryptosystems and Evolutionary DES*. Chinese Journal of Computers. 2003; 26(12): 1678-1684.
[13] ZHANG Lei, WU Wen-Ling. Rectangle and Boomerang Attacks on DES. *Journal of Software.* 2008; 19(10): 2659-2665.
[14] Yong Zhang, Jiali Xia, Peng Cai, Bin *Chen.Plaintext Related Two-level Secret Key Image Encryption Scheme*. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2012; 10(6): 1599-1607
[15] Kang Chunying. Research on generation algorithm of network two-dimensional code. *Journal of Natural Science of Heilongjiang University*. 2009; 26(2): 216-219.
[16] Li Xudong. *Image processing and application based on Android mobile terminal camera*. China: University of Electronic Science and technology. 2011.
[17] Lv Tao.*The encryption algorithm of QR code and its application in material intelligent sampling*. China. Taiyuan University of Technology. 2012.
[18] Qi Xiaoli. *Research and application of encoding and decoding for matrix 2D bar code*. China: Chongqing University. 2007.
[19] Yang Jiali. *Study of QR code recognition algorithm. Jiangnan. Jiangnan University*, China. 2011.