# A Novel Secret Sharing Technique Using QR Code

**Jun-Chou Chuang** lzchung@pu.edu.tw
*Assistant Professor*
*Department of Computer Science and communication Engineering*
*Providence University 200 Chung-Chi*
*Rd., Taichung, Taiwan*

**Yu-Chen Hu** ychu@pu.edu.tw
*Professor*
*Department of Computer Science and Information Management*
*Providence University 200 Chung-Chi*
*Rd., Taichung, Taiwan*

**Hsien-Ju Ko** nhjko@asia.edu.tw
*Assistant Professor*
*Department of Photonics and Communication Engineering*
*Asia University 500, Liufeng Rd.,*
*Wufeng, Taichung, Taiwan*

## Abstract

Any mobile device with capture function can read content from a barcode tag directly. When a barcode contains important data or privacy information, the risk of security becomes an important problem. In this paper, the QR code is employed to design the secret sharing mechanism so that the data privacy during data transmission can be enhanced. The secret data is divided into some shadows by the secret sharing mechanism and the results are embedded into barcode tags. The secret can be recovered only when the number of shadows is greater than or equal to the predefined threshold. In sum, the proposed technique improves data security for data transmission.

**Keywords:** Barcode, secret sharing, QR code.

## 1. INTRODUCTION

Barcode provides a convenient way [2][5][15] for people labeling a tag on a product so that people can easily and quickly identify the content of product itself. It can be classified into two types, one-dimensional (1D) barcode and two-dimensional (2D) barcode. The 1D barcodes use different width of lines and spaces to represent data, for example, code 39, code 128, EAN-13, EAN-128, ISBN, and etc. As for the 2D barcodes, they use symbol types of stacking and matrix to represent data, such as QR code [4][7][8][16][17][18], PDF417, Data Matrix, Maxi Code, and etc. Table 1 shows different types of 1D barcodes and 2D barcodes.

In generally, 1D barcodes put emphasis on “product identification” and 2D barcodes put emphasis on “product descriptions”. Because of the limitation of 1D barcode storage, only a few data like product identification is stored in 1D barcode. 2D barcodes are superior to that 1D barcode in embedding payload, error resistance, data security, and readability. In the storage size, 2D barcode can store a lot of information like product descriptions, including product ingredient, product item, product details, web links, and etc. For error resistance, 2D barcodes can defense different levels of error occurs.

The security of 1D barcodes is lower than 2D barcodes. 1D barcodes are very easy to read by scanning the lines and the spaces. However, 2D barcodes are not easy to read a symbol pattern by human eyes. With regard to readability, 1D barcodes must scan along a single directional. If the angle of a scan line does not fit within a range, the data would not be read correctly. However, 2D barcodes get wide ranges of angles for scanning. Thus, 2D barcodes are readability.

2D Barcodes provide a unique identifier for objects and applications [1][9][10][11] [12][13][14][15] to automatic checkout system, commerce, industry, hospital, and etc. Barcodes are very convenience to automatic systems, but they have data privacy weakness. A reader device with video capture function can read the content from tags directly. When barcodes contain privacy information may result in the risk of security issue. Therefore, the confidential data is often stored in the back-end database. When a reader captures a tag, it only gets a network link from a tag and later connected to the back-end database through the Internet. A user who has access right can login database to retrieve the privacy information.

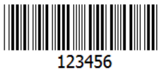
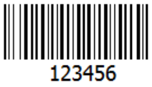
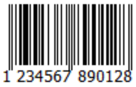
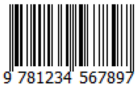
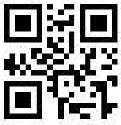
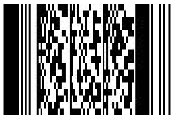
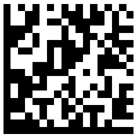
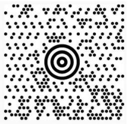
| | | | | |
|---|---|---|---|---|
| 1D barcodes | Code 39<br><br> | Code 128<br><br> | EAN-13<br><br> | ISBN<br><br> |
| 2D barcodes | QR Code<br> | PDF417<br> | DataMatrix<br> | Maxi Code<br> |

**TABLE 1:** 1D Barcodes and 2D Barcodes.

To enhance security of data privacy [3] of barcodes, we design a secret sharing technique with Quick Response code (QR code). The technique shares a confidential data into shadows and one shadow is embedded into one carrier tag. Anyone cannot recovery the original secret data from its own share. The secret can be recovered only when the number of shadows is larger than or equal to a threshold. The proposed technique does not need to connect the back-end database through Internet. Thus, the proposed technique can save much more hardware cost and can reduce the security risks transmission on the open environment.

The rest of this paper is organized as follows. In Section 2, we review the QR code. The proposed technique is described in Section 3. The security analysis and performance is listed in Section 4. Finally, the conclusions are presented in Section 5.

## 2. QR CODE

The QR code is a kind of matrix symbol, which was developed by the Japanese company Denson-Wave in 1994. Figure 1 shows the basic structure of QR code. They are quiet zone, position detection patterns, separators for position detection patterns, timing patterns, alignment patterns, format information, version information, data, and error correction codewords. They are shown in Figure 1. Some details of QR code can be refereed to [17].

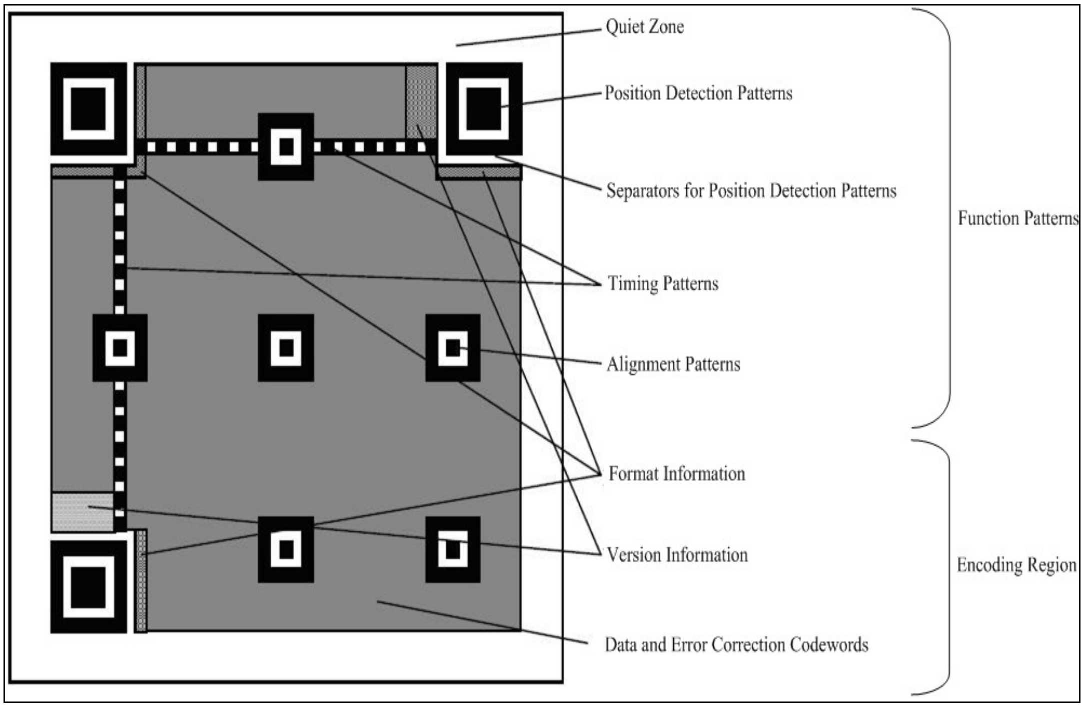


**FIGURE 1:** The basic structure of QR Code.

The main features of QR code contain large capacity, small printout size, high speed scanning, advanced error correcting, and freedom direction scanning. The overall are summarized as follows.

- High data capacity: QR code can store 7,089 numeric characters and 4,296 alphanumeric characters, and 1,817 kanji characters.
- High speed scanning: A mobile phone with camera function can get the content from a barcode quickly and easily.
- Small printout size: QR Codes carry data on both horizontally and vertically, thus QR codes are better than 1D barcodes in data capacity.
- Advance error correcting: Even if 50% areas of barcode are damaged, QR codes still can be recognized correctly.
- Freedom direction scanning: The scanning direction of QR code is freedom.

## 3. DESIGN OF SECRET SHARING TECHNIQUE USING QR CODE

The proposed technique designs a secure data transmission scheme based on the secret sharing scheme with QR code. Secret sharing scheme was first proposed by Shamir in 1979 [14]. The main idea of the secret sharing scheme divides a secret into *n* shadows or called shares. Anyone can not decrypt the original secret from their own share. The secret can be recovered only when any of *t* out of *n* shadows (*t*<=*n*) are hold together. The framework of the proposed scheme is listed in Figure 2.

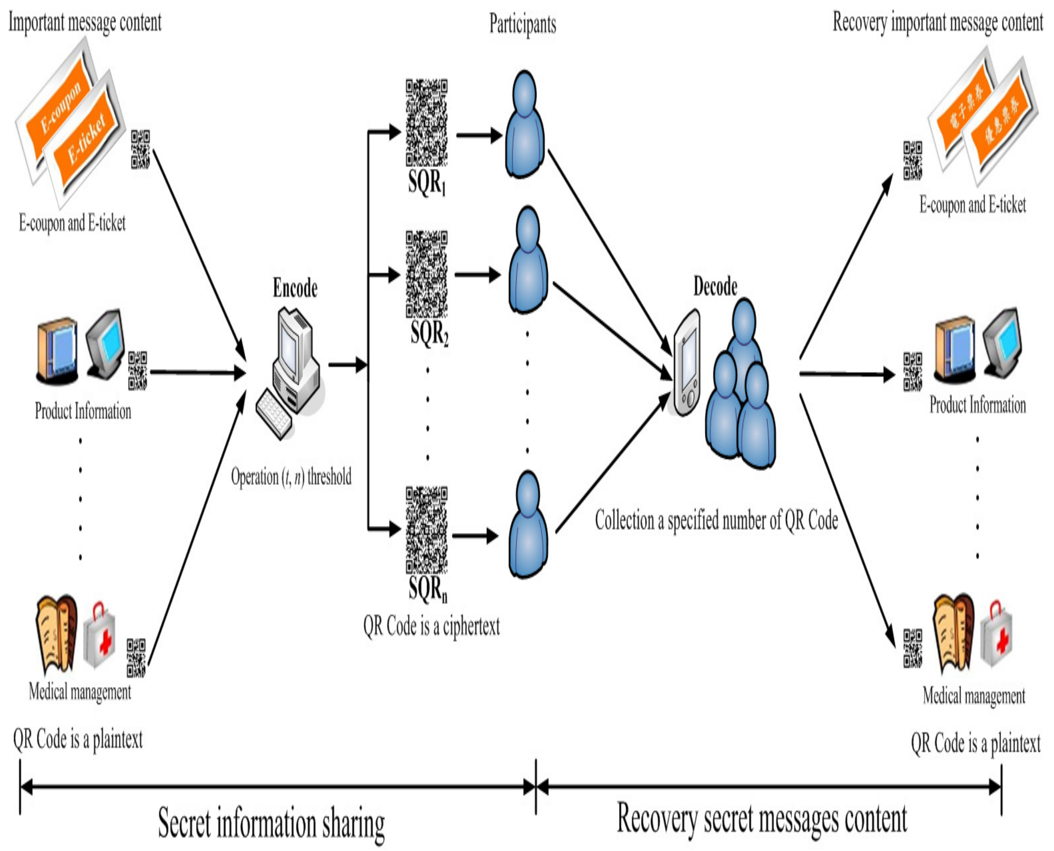


**FIGURE 2:** The framework of the proposed scheme.

In the proposed scheme, we first choose a value $t$ ($t<=n$) and a secret key $a_0$ and a large prime number $p$ ($p>=a_0$). Next, we select $n$ participants $x_1$, $x_2$, ..., $x_n$, where $n$ is the number of QR code tags, which used to be hidden. Next, a ($t$-1) degree polynomial $f(x)$ was constructed as follows:

$$f(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_{t-1} x^{t-1} (\text{mod } p) \tag{1}$$

Where $a_1$, $a_2$, …, $a_{t-1} \in Zp$. So, we can generate a pair of secret share ($x_i$, $f(x_i)=y_i$) to each participant.

In the decoding procedure, anyone who gets $t$ out of $n$ secret shares would recovery secret data $a_0$ by the Lagrange polynomial interpolation which was listed as belows.

$$f(x) = \sum_{a=1}^{t} y_{ia} \prod_{j=1, j\neq a}^{t} \frac{x - x_{ij}}{x_{ia} - x_{ij}} (\text{mod } P) \quad . \tag{2}$$

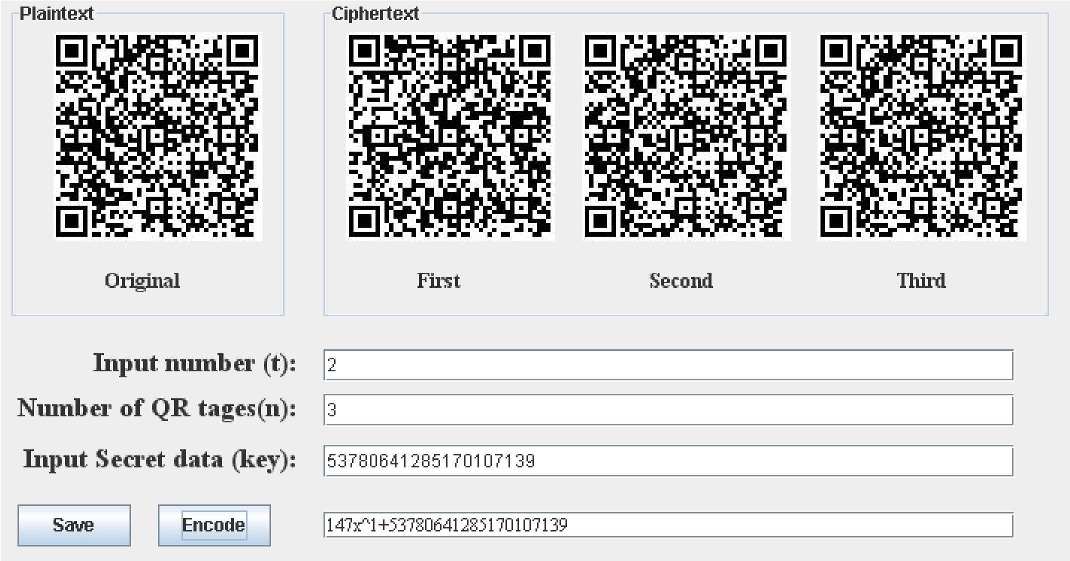
Here we illustrate an example to show how to construct secret shares. Let $t$ value is 3, $n$ value is 6, secret key $a_0$ is 1234 and the prime number $p$ is 1237. Then a ($t$-1) degree polynomial $f(x)=94x^2+166x+1234$ is constructed. Assume $x_1=1$, $x_2=2$, $x_3=3$, $x_4=4$, $x_5=5$, and $x_6=6$, we can obtain six secret shares where $f(x_1)=f(1)=1494$, $f(x_2)=f(2)=1942$, $f(x_3)=f(3)=2578$, $f(x_4)=f(4)=3402$, $f(x_5)=f(5)=4414$, and $f(x_6)=f(6)=5614$. To recover the secret key $a_0$, we need to collect three or more secret shares. Assume we obtain three secret shares, they are ($f(2)$, 1942), ($f(4)$, 3402), ($f(5)$, 4414). Then the secret key $a_0=1234$ can be decoded by the Lagrange polynomial interpolation as below.

$$f(x) = 1942(\frac{x-4}{2-4} \times \frac{x-5}{2-5}) + 3402(\frac{x-2}{4-2} \times \frac{x-5}{4-5}) + 4414(\frac{x-2}{5-2} \times \frac{x-4}{5-4})$$
$$= 1942 \times (\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}) + 3402 \times (-\frac{1}{2}x^2 - \frac{7}{2}x - 5) + 4414 \times (\frac{1}{3}x^2 - 2x + \frac{8}{2})(\bmod 1237)$$
$$= (94x^2 + 166x + 1234) \bmod 1237$$

## 4. SECURITY ANALYSIS AND PERFORMANCE

This section describes the security and the performance of the proposed scheme. The proposed scheme is based on Shamir's secret sharing scheme. The secret data is divided into shares of shadows by secret sharing technique. The generated shadows are embedded into each QR-code tag. Anyone who wants direct to read the content from QR codes is impossible if the number of received shadows is not achieved the predefined threshold. As the result, our scheme is secure.

In Figures 3-6, the share generate and the message recovery for the (2, 3)-threshold and the (3, 3)-threshold are listed below. The plaintext is divided into three shares by secret sharing technique, and then embedding them into QR codes. The decoding procedure in the (2, 3)-threshold, the original plaintext can be recovered only if the number of the received QR codes is larger than or equal to two. As for the (3, 3)-threshold, the number of the received QR codes should be equal to three. Besides, error recovery from any of two barcode tags using (3, 3)-threshold is listed in Figure 7. Because of the number of the retrieved shares is less than the predefined threshold thus the reconstructed secret key is not correct.



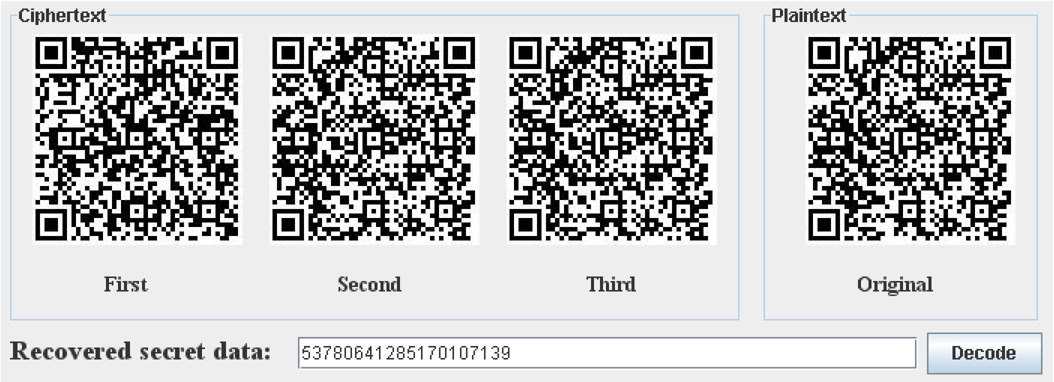
Input number (t): 2

Number of QR tages(n): 3

Input Secret data (key): 53780641285170107139

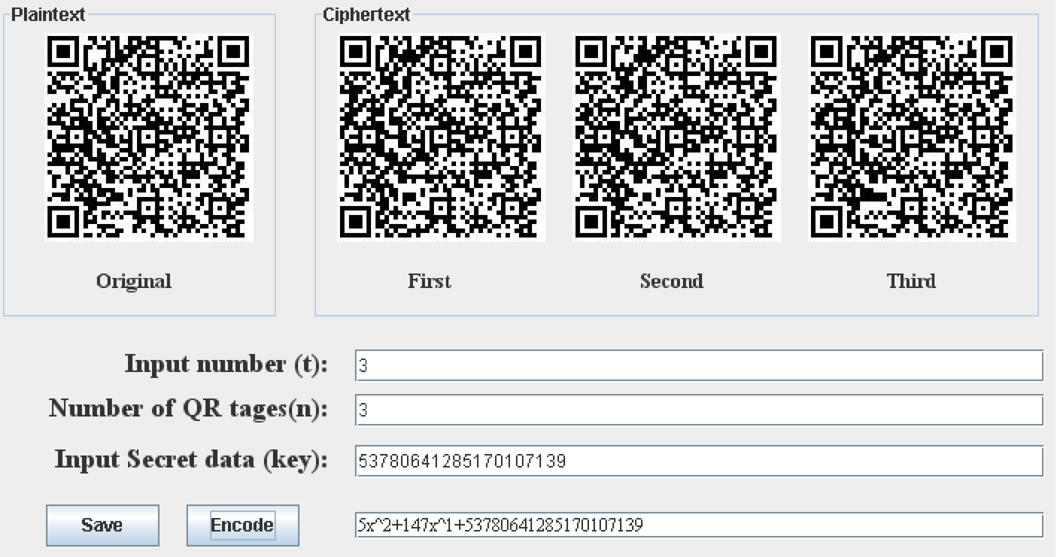
147x^1+53780641285170107139

**FIGURE 3:** Generating three secret shares using (2, 3)-threshold.



Recovered secret data: 5378064128517010 7139

**FIGURE 4:** Recovery of secret message from any of two barcode tags using (2, 3)-threshold.



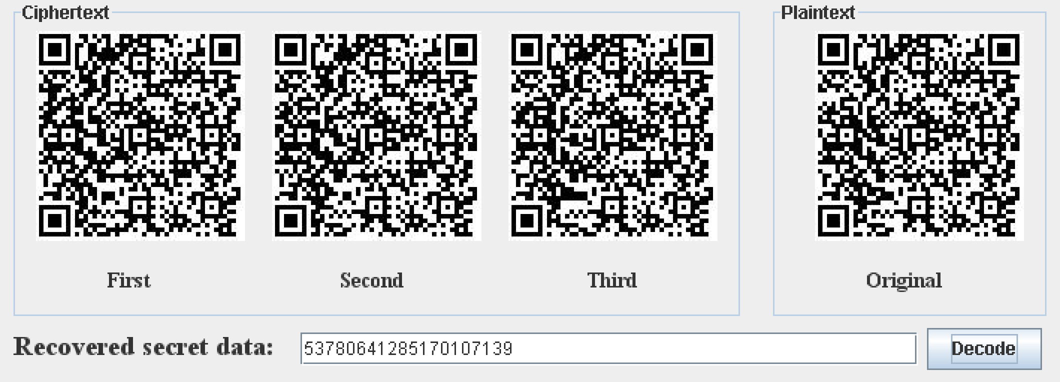
Input number (t): 3

Number of QR tages(n): 3

Input Secret data (key): 5378064128517010 7139

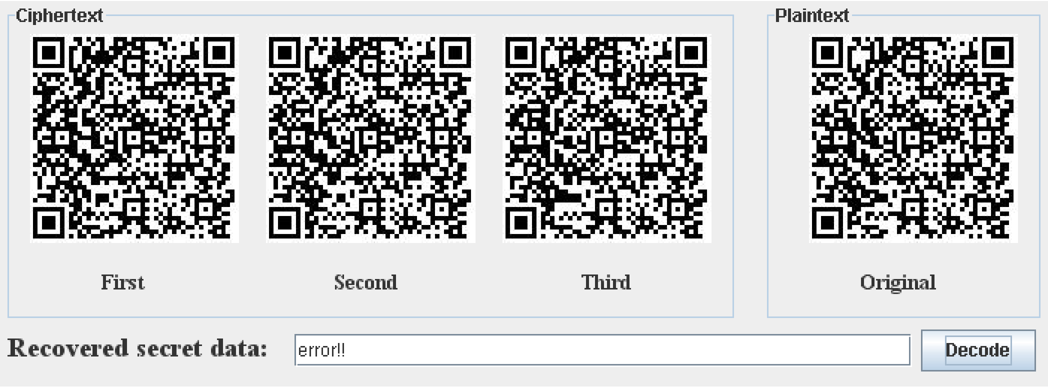
5x^2+147x^1+5378064128517010 7139

**FIGURE 5:** Generating three secret shares using (3, 3)-threshold.



Recovered secret data: 5378064128517010 7139

**FIGURE 6:** Recovery of secret message from three barcode tags using (3, 3)-threshold.



Recovered secret data: error!!

**FIGURE 7:** Error recovery from any of two barcode tags using (3, 3)-threshold.

As for our system perforamnce, our system does not need to establish a remote database for QR code data searching. Meanwhile, the proposed scheme embeds the data into QR code tags directly. The cost of this paper is only tags and printing ink. Thus, the proposed scheme can save a lot of system cost.

## 5. CONCLUSIONS

In this paper, a secret sharing mechanism to enhance the security and data privacy for QR code is proposed. The proposed technique improves data security during data transmission. On the other hand, the proposed technique does not need to establish a back-end database beforehand for contents searching. It direct embeds the secret data into tags therefore the proposed technique can save a lot of hardware cost and software maintenance. The proposed technique can be applied to some applications such as electronic tickets, airline luggage inspection, medical e-health system, and others fields.

## 6. ACKNOWLEDGMENT

The authors gratefully acknowledge the support provided to this study by the National Science Council of Taiwan under grant number NSC99-2221-E-126-006.

## 7. REFERENCES

1. H. S. Al-Khalifa, “*Mobile SRS: a classroom communication and assessment service*”. In Proceedings of the Innovations in Information Technology, United Arab Emirates, 2008.

2. T. Bouchard, M. Hemon, F. Gagnon, V. Gravel, and O. Munger, “*Mobile telephones used as boarding passes: Enabling Technologies and Experimental Results*”. In Proceedings of the 4th Autonomic and Autonomous Systems, Gosier, Guadeloupe, 2008.

3. T. Chen, “*The application of bar code forgery - proof technology in the product sales management*”. In Proceedings of the Intelligent Information Technology Application Workshops, Washington, DC, USA, 2008.

4. U. B. Ceipidor, C. M. Medaglia, and A. Perrone, M. D. Marsico, and G. D. Romano, “*A museum mobile game for children using QR-codes*”. In Proceedings of the 8th International Conference on Interaction Design and Children, Italy, 2009.

5. Y. J. Chang, S. K. Tsai, and T. Y. Wang, “*A context aware handheld wayfinding system for individuals with cognitive impairments*”. In Proceedings of the 10th international ACM SIGACCESS conference on Computers and accessibility, Halifax, Nova Scotia, Canada, 2008.

6. N. Fujimura and M. Doi, "*Collecting students' degree of comprehension with mobile phones*". In Proceedings of the 34th Annual ACM SIGUCCS Conference on User Services, Canada, 2006.

7. T. Falas and H. Kashani, "*Two-dimensional barcode decoding with camera-equipped mobile phones*". In Proceedings of the Pervasive Computing and Communications Workshops, White Plains, NY, USA, 2007.

8. J. Z. Gao, L. Prakash, and R. Jagatesan, "*Understanding 2D-barcode technology and applications in m-commerce – design and implementation of a 2D barcode processing solution*". In Proceedings of the Computer Software and Applications Conference, Bejing, China, 2007.

9. T. Kamina, T. Aoki, Y. Eto, N. Koshizuka, J. Yamada, and K. Sakamura, "*Verifying identifier-authenticity in ubiquitous computing environment*". In Proceedings of the Advanced Information Networking and Applications Workshops, Ontario, Canada, 2007.

10. B. Lingyan, F. Zewei, L. Min, and W. Weining, "*Design and implementation of the airline luggage inspection system base on link structure of QR code*". In Proceedings of the Electronic Commerce and Security, Guangzhou, 2008.

11. T. Y. Liu and Y. L. Chu "*Handheld augmented reality supported immersive ubiquitous learning system*". In Proceedings of the Systems, Man and Cybernetics, Singapore, 2008.

12. J. Rouillard, "*Contextual QR codes*". In Proceedings of the 3rd International Multi-Conference on Computing in the Global Information Technology, Athens, Greece, 2008.

13. S. Reiser and R. Bruce, "*Service learning meets mobile computing*". In Proceedings of the Annual Southeast Regional Conference, Auburn, Alabama, 2008.

14. A. Shamir, "*How to Share a Secret*". Communication of the ACM, 22(11): 612-613, 1979.

15. G. Starnberger, L. Froihofer, and K. M. Goeschka, "*QR-TAN: Secure mobile transaction authentication*". In Proceedings of the Availability, Reliability and Security, Fukuoka, Japan, 2009.

16. Y. L. Yeh, J. C. You, and G. J. Jong, "*The 2D bar-code technology applications in medical information management*". In Proceedings of the Intelligent Systems Design and Applications, Kaohsiung, Taiwan, 2008.

17. ISO/IEC18004, "*Information technology-automatic identification and data capture techniques*". Bar Code Symbology - QR Code.

18. Denso-wave, http://www.denso-wave.com/qrcode/index-e.html.