Journal of Theoretical and Applied Information Technology
10th January 2016. Vol.83. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# PROTECTING WIRELESS DATA TRANSMISSION IN MOBILE APPLICATION SYSTEMS USING DIGITAL WATERMARKING TECHNIQUE

**KARTINI MOHAMED[1], FATIMAH SIDI[2], MARZANAH A. JABAR[3], ISKANDAR ISHAK[4]**

[1]SIRIM Berhad, 1, Persiaran Dato' Menteri, P.O. Box 7035,Section 2, 40700 Shah Alam, Selangor, Malaysia.

[2,3,4]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400, UPM Serdang, Selangor, Malaysia

E-mail: [1]kartinim@sirim.my, [2]fatimah@upm.edu.my, [3]marzanah@upm.edu.my, [4]iskandar_i@upm.edu.my
Corresponding author: fatimah@upm.edu.my

## ABSTRACT

There have been many cases of fake documents be used for important legal transactions. This includes the use of fake degrees or certificates during professional job applications either in private sectors or government related firms. Since many people are using smart phones currently, it is possible to have a mobile application system (apps) that can validate the correctness of legal documents or certificates in real-time basis. The apps must be able to validate the certificate by confirming it with the data obtained from a registered database owned by relevant academic institutions. However, since these data require wireless transmissions which are vulnerable to data manipulations by hackers, this paper introduces a protection measure using encrypted elements of user authentication to watermark the transmitting data. This is to ensure the data being transmitted using the mobile apps are secured from being hacked by unauthorized parties and without much time delay. To analyze the effectiveness of this watermarking technique, a special mobile apps is developed. The effectiveness of the technique is measured in terms of the correctness of the data before and after being transmitted, the time taken to process the data before and after being transmitted and the processing time increment rate versus the data size increment. From this experiment, not only the correctness of the certificate could be confirmed instantly but also the transmitted data are well protected without much data processing delay. This indicates that the proposed watermarking technique is effective to ensure the data are well protected during wireless transmission and therefore users can conveniently use the apps to immediately detect fake degrees.

**Keywords***:* *QR Code, Digital Watermark, Data Transmission, Wireless Communication, Mobile Application Systems*

## 1. INTRODUCTION

It has been reported in Malaysian newspapers and online news recently that several cases of those having important posts have used fake degrees for securing their jobs not only in government firms but also in private sectors. An online news reported on 27th July 2012 that the local police department had discovered 525 'graduates' who were ‘without attending lectures, sitting for examination and submitting papers’. The fake degrees were believed to be issued by 5 foreign universities in which three of these universities were non-existence. The degrees were sold at RM6500.00 for Bachelor of Science, RM8500.00 for Masters and RM10500.00 for a PhD [1].

The Star online news dated 3rd October 2013 reported that the government needed a new law to rule out fake degrees. It was because the Malaysian Parliament had highlighted that 2 cases of fake degrees were detected in Public Service Commission between 2007 till 2012 [2].

The online New Straits Time news revealed on 7th September 2012 that a 'lecturer' had used fake degrees from the United States and Canada to work as a university lecturer for two years before becoming a consultant in a government department [3].

Moreover, there are several portals that are selling fake degrees online which produce degree certificates that look very similar to the genuine ones. With the selling prices affordable by many people, it is not easy to stop people from using fake degrees for their job applications.

The question now is how to ensure the use of fake degrees can immediately be identified as to prevent unqualified candidates from taking any critical jobs? Due to this concern, this paper introduces a method to detect fake degrees instantly using a secured mobile apps together with degree certificates printed with QR (Quick Response) Codes.

QR Code has been widely used for data communication after it was introduced in 1994 by a Japanese company known as Denso Wave. It was initially used for marketing purposes but was recently used in medical [4][5], financial [6][7], business and marketing purposes [8][9], educations [10][11][12]and government affairs [13][14][15] in many countries all over the world. QR Code is a square shape of 2-dimensional barcode which has higher data capacity compared to the traditional 1-dimensional barcode. It can carry data up to 7089 numeric characters, 4296 alphanumeric characters, 2953 binary bytes and 1817 Kanji characters [10]. With this capacity, it can be used to carry large information such as URL, contact numbers, email addresses, animations links, etc. [16]. It can be encoded using free online QR Code generators and easily decoded using free applications available in most smart phones or devices.

The use of QR Code's image on degree certificates and a special mobile scanning software, can identify the legitimacy of the certificates easily. The QR Code image must carry information or attributes as printed on the certificate such as the name of the degree holder, the name and address of the institution issuing the degree, the date of degree issuance and the field name of the degree. Using a special scanning software, data carried by a QR Code's image are retrieved by the phone that will compared with the corresponding data obtained from a database of the registered degrees. The degree certificate can be considered as genuine if these 2 sets of data match.

However, the above system requires data to be wirelessly transmitted. Unfortunately, data being communicated wirelessly or through mobiles are not secured and very vulnerable to security attacks [17]. Thus, it is important to ensure transmitted data be safe from these attacks. Researchers have proposed many ways to protect data transmission in mobile or wireless communications such as by using secured data/document [18][19], secured storage/database [20][21], secured network [22][23] strong user authentication [24][25] and reliable device/network service [26][27]. Even though each of them has their own advantages and disadvantages, this paper has chosen the improvement in terms of secured data/document as a start since the degree certificates may contain confidential data that needs to be protected.

To secure data/document, many improved security or protection measures have been introduced by researchers. For example, [18] and [19] have suggested on the use of symmetric-key operations to encrypt the data, [28] proposed the use of secure fingerprints using QR Codes, [29] proposed the change of the security protocols used between two peers, [30] focused on the secured watermarks to detect false injection attack, [31] highlighted the use of Visual Secret Sharing (VSS) scheme while [32] recommend the use of watermark in Wireless Sensor Network and [33] suggested the use of digital watermark and signature to secure the data. However most of these improvement depends only on one type of protection measure. Besides, no analysis has been done to see if the processing time and its increment rate are not badly affected when the proposed improvements are being applied. This is because the user might not want to use the system if the processing time is too long and the users could not afford to waste more times.

Taking into the above consideration, this paper proposes a technique of making data transmission be well protected by applying watermarks of encrypted user authenticating data while ensuring no big delay in data processing time.

To test the effectiveness of this watermarking technique, a similar experiment has been carried out for a QR Code used to verify the legitimacy of a personal identification card called 'MyID' card. This paper actually improvises the experiment that has been previously done in 2013 [34].

Section 2 of this paper talks about the infrastructure of the experimental system followed by section 3 which explains about the watermarking technique. Section 4 illustrates the test method, Section 5 summarizes the results and Section 6 concludes the findings and future works.

## 2. THE INFRASTRUCTURE OF THE EXPERIMENTAL SYSTEM

To construct the experimental system of using QR Codes in MyID Card, several hardware devices and software have been used. The hardware devices consist of a smart phone (Samsung Galaxy Note 3), and a laptop which displays the softcopies of MyID cards. The smart phone has been installed with a free demo version of QR Code scanner called 'Barcode Keyboard' version 1.4.1 which is able to convert the scanned data into keystrokes. The phone is also provided with a special mobile apps that can process the scanned data from QR Code and retrieve the corresponding data from a database. A special mobile apps is developed to compare these two sets of data -from QR code and from databases.

The algorithms are written using PHP language and communicating with mobiles and servers using android-sdk platform in Eclipse-Juno operating environment. The Eclipse Project version 4.2.0 release on 8th June 2012 is used for this operating environment.

For the wireless communication service, a Wi-Fi service subscribed from Telekom Malaysia Berhad - Unify package is used. Since there are many uncontrolled parameter related to data transmissions between mobiles and databases such as traffic congestions due to bad quality of service, distance of communications, time of usage, etc. the algorithms and the database are both located in one subscribed cloud server.

## 3. THE WATERMARKING TECHNIQUE

The proposed data for watermark is the text-based elements of user authentication. This means the mobile apps developed for this study requires a mobile user to do authentication. The data for user authentication are not necessary to be very complicated. It can be done by having only four text-based elements as recommended by [25] comprising username, password, mobiles' IMEI (The International Mobile Equipment Identity) number and SIM (Subscriber Identification Module) Card number. The user is required to key in username and password while the IMEI and SIM Card numbers are auto-retrieved by the mobile device. In comparison with the existing watermarking techniques done by other researchers such as [35], the user authenticating data is normally used once during the initial authorization process whereas the proposed watermarking technique reuses the user authenticating data for data protection during their transmission as illustrated in Figure 1.

Figure 2 shows how a user needs to key-in the username and password for the authentication. The IMEI and SIM Card numbers are not displayed on screen but they are auto-retrieved by the background operation. All user authenticating data are then combined, encrypted, and blended to form a digital watermarking data. Meanwhile each attribute of information from QR Code is also encrypted individually. The watermarking data from user authenticating data are then chunked into smaller number of digits (represented by $W_1$, $W_2$, $W_3$, …, $W_n$) and each is appended to each attributes of QR Code's data ($D_1$, $D_2$, $D_3$, …, $D_n$). These appended numbers are combined into $W_1D_1$, $W_2D_2$, $W_3D_3$, …, $W_nD_n$ and transmitted from mobiles to server to search for the corresponding data or records in a database. Once the corresponding records (represented by $R_1$, $R_2$, $R_3$, …, $R_n$) are obtained, they are combined one more time before they are transmitted back to the mobile devices as $W_1D_1R_1$, $W_2D_2R_2$, $W_3D_3R_3$, …, $W_nD_nR_n$ as demonstrated in Figure 3.

Once these data arrive to mobile device, the watermarked data are detached so that the data comparison between QR Code's ($D_1$, $D_2$, $D_3$, …, $D_n$) and database ($R_1$, $R_2$, $R_3$, …, $R_n$) can be done. Before the results of comparison can be displayed on mobile's screen as shown in Figure 4(a) or Figure 4(b), the user is required to re-authenticate to ensure only the right users and mobile devices receive the data. The results displayed in Figure 4(a) are 'without violation' which means QR Code's data match with database's data. On the other hand, if they are not matched, Figure 4(b) will be displayed to indicate that they have violations. A violation is detected as in Figure 4(b), due to inconsistency of Date of Birth of 'MyID' card holder. An example of MyID card with QR Code used in this experiment is as in Figure 5.

## 4. THE TEST METHOD

Two mobile apps are developed to measure the effectiveness of the proposed watermarking technique in which one of the apps is used as a reference sample. Both apps are using the user authenticating data as proposed by [25] but one is not using any watermarking technique (referred as an existing technique or reference sample) and the other is using the watermarking technique (the proposed technique) as summarized in Table 1.

The mobile apps are developed to be able to scan QR Codes on MyID cards, search the relevant records in databases and perform the comparisons to check if inconsistencies exist between data obtained from scanning QR Code and those from databases. The card is considered as fake if any inconsistencies are detected between these 2 sets of data.

Tests are done to measure the processing time, data integrity and the relation between processing time and different sizes of data. The processing time is measured when the data are encrypted, attached, blended, unblended, detached and decrypted, before and after the data are communicated between mobile devices and databases. As a basic start, the data encryption method used in this study is binary encryption method as introduced by ISO/IEC 18004 [36]. However, it could also be done using other encryption types including the one proposed by [37] which has been tested to protect wireless data transmission. 50 sets of QR Codes have been used and was tested repeatedly until the results give a stable average processing time. A sub-program is developed to run and record the average processing times for each of both systems with and without the proposed watermarking technique.

The improved performance of data integrity is measured based on the percentage of data loss or corrupted between input (QR Code's data) and expected final output (data to be displayed on mobile's screen). Data integrity is considered as improved if there are no discrepancies between these two sets of data while using the proposed protection measure. To effectively measure the differences of these sets of data, a hash function is applied. In this experiment, SHA-384 is used for the comparison since it is one of the hash functions under SHA-3 level, the highest level of hash functions recognized by the National Institute of Standards and Technology (NIST). For easy understanding of the percentage of data loss or corrupted, zero data loss means 100% of data accuracy which indicates good data integrity. To measure and record the results of these comparison, a different sub-program is developed to compare the input and the output data using SHA-384 hash function.

The trend of processing time vs. data sizes is also analyzed to find out the behavior of processing time towards different data sizes. This is done because it is also important to know whether the processing time is increasing exponentially or linearly with the increased data size. Linear increment is preferred because it means the processing time is slowly increasing when the size of data increases. The graph of this processing time based on the number of characters in each QR Code's data is plotted to find out the trend of processing time versus data sizes.

## 5. RESULTS AND DISCUSSION

This section summarizes the results and discussions related to the data integrity, processing time as well as the graph of processing time vs. data size.

a) Data integrity

To determine good data integrity, it is vital to ensure all expected final output data are consistent with input data. Tests were done for 50 MyID card numbers and each card is provided with one QR Code's data consisting of 10 attributes - MyID number, name, address, county, city, state, zip code, date of birth, gender and race. Based on 50x10 or 500 number of attributes, the results (as indicate in Figure 6 show that there is zero percent of data error between the 'input' and 'actual output' data which means data integrity achieves 100% accuracy.

b) Processing Time

Processing Time is recorded for 50 MyID cards in which each card is tested for 25 times for those systems with and without the proposed watermarking technique. The results which are plotted into a graph as shown in Figure 7 indicate that the average processing time converges to be similar after 21 times running for 50 MyID cards. This means the time taken to run the system with and without the proposed watermarking technique are not much different after running for a certain number of times.

c) Processing Time vs. Data Size

To measure the time performance of the proposed watermarking technique which involves the process of watermarking, de-watermarking, encryption and decryption, a graph is plotted for the systems with and without the proposed watermarking techniques as illustrated in Figure 8. Calculating using Microsoft Excel Sheet, it seems that the time delay increases linearly based on the number of characters or data size. This is good because linear increment means the system is controllable compares to those that increase exponentially as achieved by [35], as an example.

## 6. CONCLUSION

Due to many fake degree certificates being used for job applications in the country which may allow unqualified candidates taking critical jobs with critical responsibilities, it is important to have a secured mobile apps that can detect the used of these degrees in real time basis. One of the solutions to detect fake certificates instantly is by using a special designed mobile apps as proposed in this paper. However, mobile apps require wireless data transmissions which are vulnerable to data manipulations by hackers. This will cause data integrity be jeopardized and as a result users will be reluctant to use this mobile apps. One of the ways to gain users' confident in using this apps is to ensure data are protected using the proposed watermarking technique. The technique is applied to ensure data integrity is 100% accurate where no personal or sensitive data be changed or altered during their transmissions between mobiles and related databases. Experiments were carried out to measure the accuracy of data being transmitted and the time taken to process the watermarking technique. Results show that the proposed watermarking technique is good and acceptable since it does not cause much delay in processing time with reasonable processing time's increment rate vs. data size increment while ensuring the data being wirelessly transmitted are well protected. In future research, the watermarking data will be encrypted using different encryption types and the elements of user authentication will be enhanced. Tests will be done to evaluate the level of protections given by different watermarking data.

## 7. ACKNOWLEDGEMENT

This work is financially supported by Universiti Putra Malaysia, grant no. 05-02-12-2160RU.

## REFERENCES

[1] *"Police tracking 'Tan Sri' in fake degree probe"*. (2012). Retrieved from http://www.theborneopost.

[2] *"Parliament: Fake degrees - new laws needed"*. (2013). Retrieved from http://www.thestar.com.my/News/Nation/2013/10/03/Fake-degrees-new-laws-needed-Action-taken-now-only-if-its-used-in-civil-service.aspx.

[3] *"Fake degrees land him plum jobs"*. (2013). Retrieved from Fake degrees land him plum jobs - Top News - New Straits Times http://www.nst.com.my/top-news/fake-degrees-land-him-plum-jobs-1.139103#ixzz2nnOyO6bX.

[4] Ko, E., Ju, J. S., & Kim, E. Y. (2011). Situation-based Indoor Wayfinding System for the Visually Impaired. *The proceedings of the 13th international ACM SIGACCESS conference on Computers and accessibility, ASSETS '11*, (pp. 35-42).

[5] Dixon, J. L., Smythe, W. R., Momsen, L. S., Jupiter, D., & Papaconstantinou, H. T. (2013, Feb). Quick Response Codes for Surgical Safety: A Prospective Pilot Study. *Journal of Surgical Research, 184*, pp. 157-163.

[6] Suryotrisongko, H., Sugiharsonob, & Setiawan, B. (2012). A Novel Mobile Payment Scheme Based on Secure Quick Response Payment with Minimal Infrastructure for Cooperative Enterprise in Developing Countries. *International Congress on Interdisciplinary Business and Social Science 2012 (ICIBSoS 2012).65* , pp. 906 – 912. Procedia - Social and Behavioral Sciences.

[7] Gao, J., Kulkarni, V., Ranavat, H., Chang, L., & Mei, H. (2009). A 2D Barcode-Based Mobile Payment System. *Third International Conference on Multimedia and Ubiquitous Engineering*, (pp. 320-329).

[8] A-Lin, R., Yuan, F., & Ying, G. (2011). QR code image detection using run-length coding.

*Internatonal Conference on Computer Science and Network Technology*, (pp. 2130-2134).

[9] Anand, R., Regan, R., & Mohanraj, V. (26th-28th July 2012). Cloud Based Shopping Guide System using QR Code. *ICCCNT'12.* Coimbatore, India: IEEE-20180.

[10] Law, C., & So, S. (2010). QR Codes in Education. *Journal of Educational Technology Development and Exchange, 3* (1), 85-100.

[11] Susono, H., & Shimomura, T. (2006). Using Mobile Phones and QR Codes for Formative Class Assessment. *Current Developments in Technology-Assisted Education* , 1006-1010.

[12] Chaisatien, P., & Akahori, K. (2007). A Pilot Study on 3G Mobile Phone and Two Dimension Barcode in Classroom Communication and Support System. *Seventh IEEE International Conference on Advanced Learning Technologies (ICALT 2007)* (pp. 111-113). IEEE.

[13] Jevremovic, V., & Petrovski, S. (2012). MUZZEUM - Augmented Reality and QR Codes Enabled Mobile Platform with Digital Library, used to Guerrilla Open the National Museum of Serbia. 561-564.

[14] Finzgar, L., & Trebar, M. (2011). Use of NFC and QR Code Identification in an Electronic Ticket System for Public Transport. *19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, (pp. 1-6).

[15] Li, D., Wang, Y., Hu, L., Li, J., Guo, X., Lin, J., et al. (2010). Client/Server Framework-Based Passenger Line Ticket System Using 2-D Barcode on Mobile Phone. *International Conference on E-Business and E-Government*, (pp. 97-100).

[16] Ono, S., & Nakayama, S. (Dec. 15-17, 2010). A System for Decorating QR Code with Facial Image Based on Interactive Evolutionary Computation and Case-Based Reasoning. *Second World Congress on Nature and Biologically Inspired Computing*, (pp. 401-406). Kitakyushu, Fukuoka, Japan.

[17] Gordon, M., & Sankaranarayanan, S. (2010). Biometric Security Mechanism in Mobile Payments. *IEEE* .

[18] Isaac, J. T., Zeadally, S., & Sierre, J. C. (2010). Implementation and performance evaluation of a payment protocol for vehicular ad hoc networks. *Electron Commer Res* .

[19] Pandey, P. P., Pandey, V., & Sinha, S. K. (2013). An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security. *International Journal of Computer Applications, 74* (20), pp. 29-33.

[20] Meena, S., & Daniel, E. &. (2013). Surveyon Various Data Integrity Attacks in Cloud Environment and the Solutions. *International Conference on Circuits, Power and Computing Technologies [ICCPCT]* , 1076-1081.

[21] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., et al. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences , 258*, 371–386.

[22] Zhou, L., & Zhang, Z. (2012). A Secure Data Transmission Scheme for Wireless Sensor Networks Based on Digital Watermarking. *9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)* , 2097-2101.

[23] Kumar, V., & Madria, S. (2013). PIP: Privacy and Integrity Preserving Data Aggregation in Wireless Sensor Networks. *IEEE 32nd International Symposium on Reliable Distributed Systems* (pp. 10-19). IEEE Computer Society.

[24] Belkhede, M., Gulhane, V., & Bajaj, P. (2012). Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach. *ICACT* , 1193-1197.

[25] Elkhhodr, M., Shahrestani, S., & Kourouche, K. (2012). A Proposal to Improve the Security of Mobile Banking Applications. *Tenth International Conference on ICT and Knowledge Engineering* (pp. 260-265). IEEE.

[26] Masrek, M. N., Uzir, N. A., & Khairuddin, I. I. (2012). Trust in Mobile Banking Adoption in Malaysia: A Conceptual Framework. *Journal of Mobile Technologies, Knowledge & Society , 2012*.

[27] Castiglione, A., Palmieri, F., Fiore, U., Castiglione, A., & Santis, A. D. (2015). Modeling energy-efficient secure communications in multi-mode wireless mobile devices. *Computer System Science* .

[28] Liu, S. Y. (2010). Anti-counterfeit system based on mobile phone QR code and fingerprint. *Second International Conference on Intelligent Human-Machine Systems and Cybernetics* , pp. 236-240.

[29] Rocha, B. P., Costa, D. N., Moreira, R. A., Rezende, C. G., Loureiro, A. A., & Boukerche, A. (2010). Adaptive security protocol selection for mobile computing. *Journal of Network and Computer Applications , 33*, 569-587.

[30] Bhattarai, S., Ge, L., & Yu, W. (2012). A Novel Architecture against False Data

Injection Attacks in Smart Grid. *Communication and Information Systems Security Symposium* , 907-911.

[31] Espejel -Trujillo A., C.-C. I.-M.-M. (2012). Identity Document Authentication Based on VSS and QR Codes. *The 2012 Iberoamerican Conference on Electronics ENgineering and Computer Science* (3), pp. 241-250.

[32] Harjito, B., Potdar, V., & Singh, J. (2012). Watermarking Technique for Copyright Protection of Wireless Sensor Network Data using LFSR and Kolmogorov Complexity. *MoMM2012* (pp. 208-217). Bali, Indonesia: ACM.

[33] Shukla, S. S., Singh, S. P., Shah, K., & Kumar, A. (2012). Enhancing Security & Integrity of Data Using Watermarking & Digital Signature. *International Conference on Recent Advances in Information Technology (RAIT).* IEEE.

[34] Mohamed, K.; Sidi, F.; Jabar, M. A.; Ishak, I.(2013). A Novel Watermarking Technique In Data Transmission Between QR Codes And Database. *IEEE Conference on Open Systems (ICOS)*, pp95 - 99, DOI:10.1109/ ICOS.2013.6735055

[35] Roy, S., & Manasmita, M. (2011). A Novel Approach to Format Based Text Steganography. *Proceedings of the 2011 International Conference on Communication, Computing & Security* , pp. 511-516.

[36] Wakahara, T., & Yamamoto, N. (2011). Image Processing of 2-Dimensional Barcode. *International Conference on Network-Based Information Systems*, (pp. 484-490).

[37] Zirra, P., & Wajiga, G. (2011). Cryptographic Algorithm Using Matrix Inversion as Data Protection. *Journal of ICT, 10*, 67-83.

*Table 1Existing Technique and Proposed Technique*

| Technique | User authentication | Protection Measure |
|---|---|---|
| Existing Technique (Elkhodr's Technique) | Username<br>Password<br>IMEI Number<br>SIM Card Number | Encryption |
| Proposed Technique (Improvised Elkhodr's Technique) | Username<br>Password<br>IMEI Number<br>SIM Card Number | Encryption + Watermark |

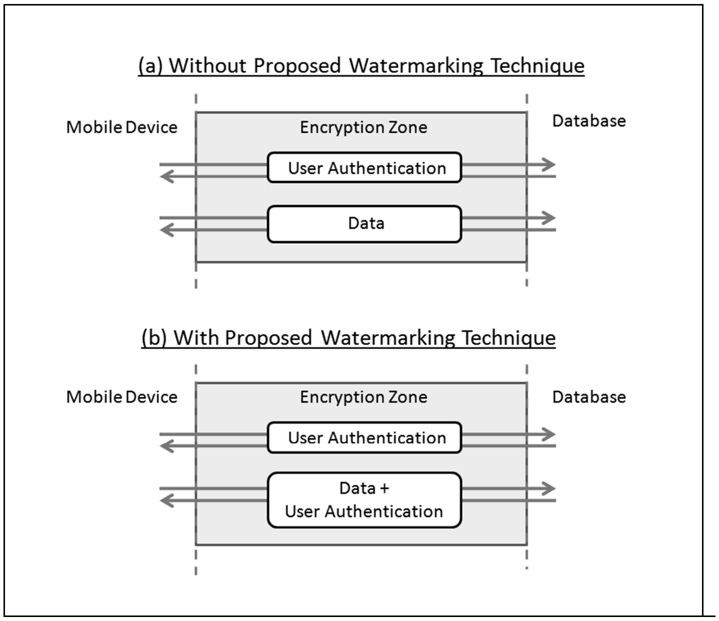
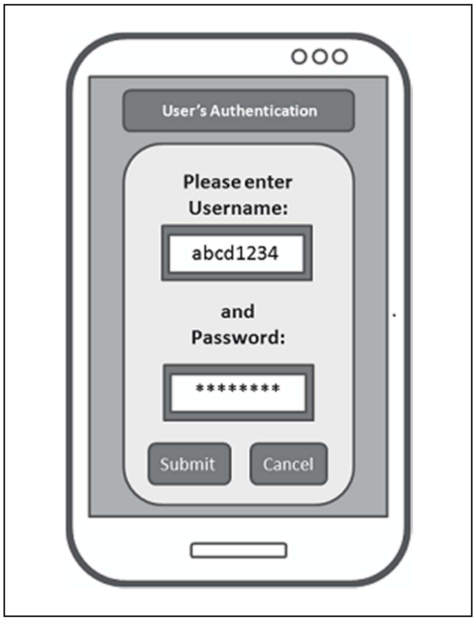


*Fig. 1 The Reuse of User authentication Information in the Proposed Watermarking Technique*



Please enter Username:

abcd1234

and Password:

********

*Fig. 2 User authentication on Mobiles*

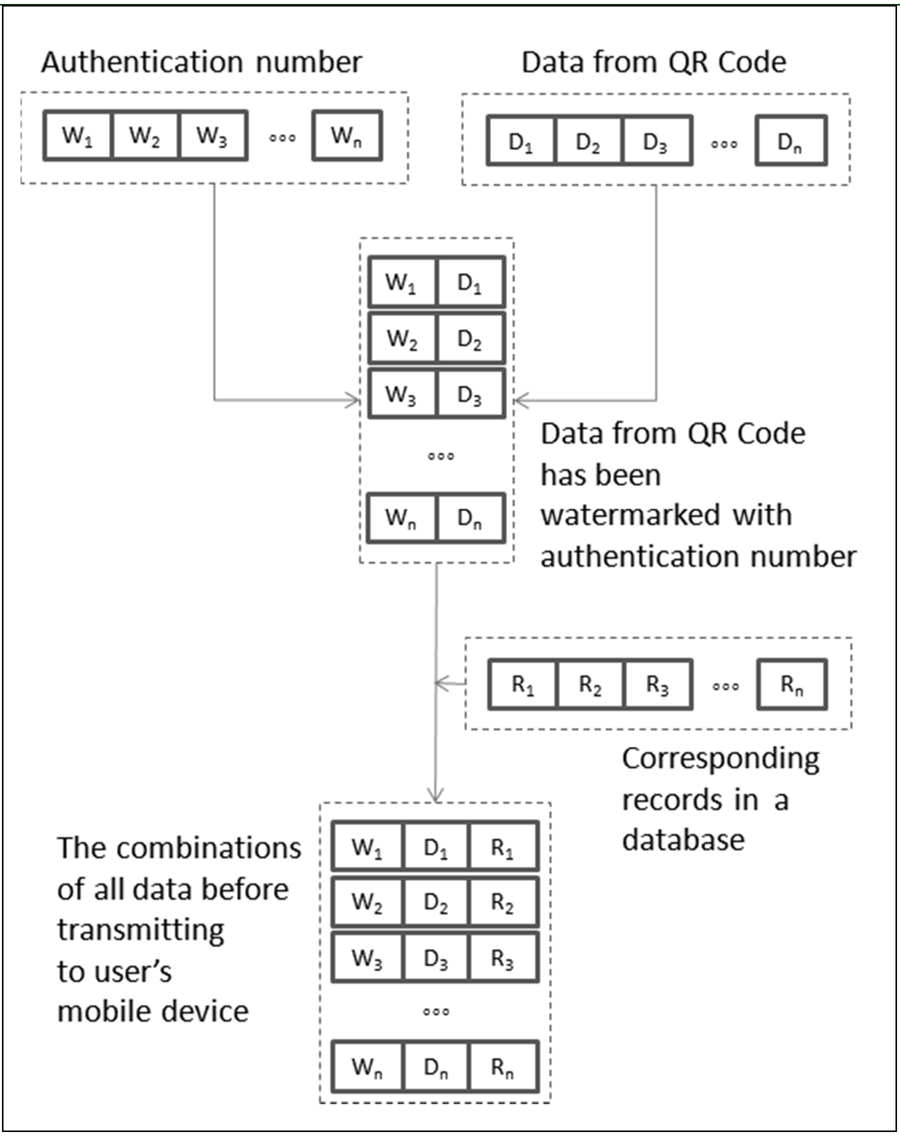
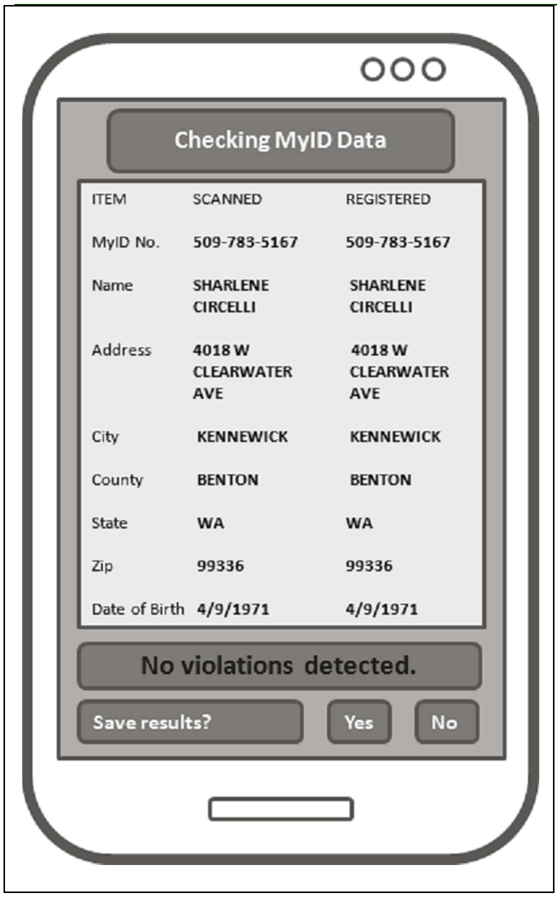

Authentication number
Data from QR Code
$W_1$ $W_2$ $W_3$ ∘∘∘ $W_n$
$D_1$ $D_2$ $D_3$ ∘∘∘ $D_n$
$W_1$ $D_1$
$W_2$ $D_2$
$W_3$ $D_3$
∘∘∘
$W_n$ $D_n$
Data from QR Code has been watermarked with authentication number
$R_1$ $R_2$ $R_3$ ∘∘∘ $R_n$
Corresponding records in a database
The combinations of all data before transmitting to user's mobile device
$W_1$ $D_1$ $R_1$
$W_2$ $D_2$ $R_2$
$W_3$ $D_3$ $R_3$
∘∘∘
$W_n$ $D_n$ $R_n$

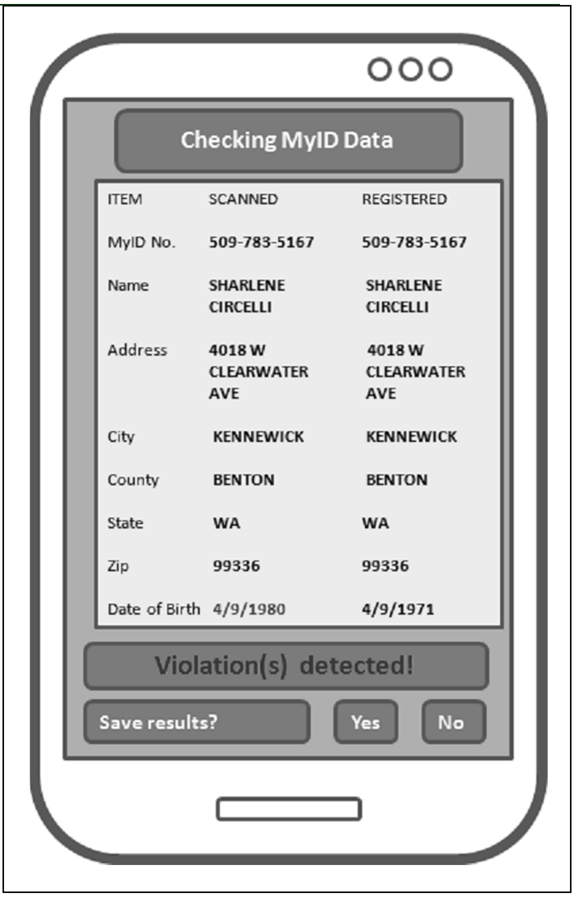
*Fig. 3 The Flow of Watermarked Data*


Checking MyID Data

| ITEM | SCANNED | REGISTERED |
|---|---|---|
| MyID No. | 509-783-5167 | 509-783-5167 |
| Name | SHARLENE CIRCELLI | SHARLENE CIRCELLI |
| Address | 4018 W CLEARWATER AVE | 4018 W CLEARWATER AVE |
| City | KENNEWICK | KENNEWICK |
| County | BENTON | BENTON |
| State | WA | WA |
| Zip | 99336 | 99336 |
| Date of Birth | 4/9/1971 | 4/9/1971 |

No violations detected.

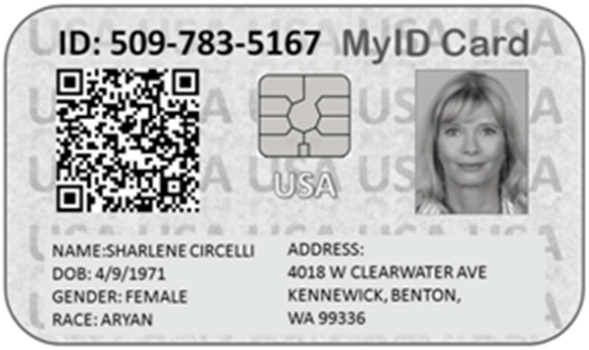
Fig. 4(a) Results without Violation


Checking MyID Data

| ITEM | SCANNED | REGISTERED |
|---|---|---|
| MyID No. | 509-783-5167 | 509-783-5167 |
| Name | SHARLENE CIRCELLI | SHARLENE CIRCELLI |
| Address | 4018 W CLEARWATER AVE | 4018 W CLEARWATER AVE |
| City | KENNEWICK | KENNEWICK |
| County | BENTON | BENTON |
| State | WA | WA |
| Zip | 99336 | 99336 |
| Date of Birth | 4/9/1980 | 4/9/1971 |

Violation(s) detected!

Fig. 4(b) Results with a Violation

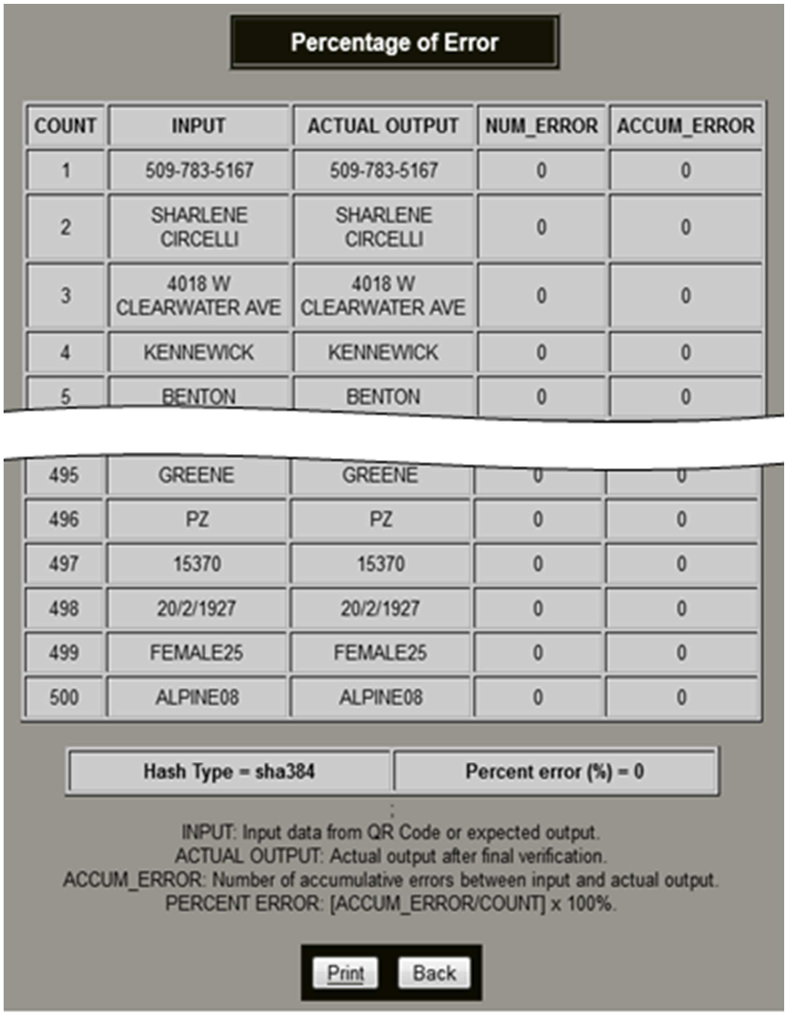

ID: 509-783-5167 MyID Card

NAME:SHARLENE CIRCELLI
DOB: 4/9/1971
GENDER: FEMALE
RACE: ARYAN

ADDRESS:
4018 W CLEARWATER AVE
KENNEWICK, BENTON,
WA 99336

Fig. 5 Sample of MyID Card[1]

[1] ID photo is taken from http://www.onlinepassportphoto.com/images/Germany_sample_passport_photo.jpg



Percentage of Error

| COUNT | INPUT | ACTUAL OUTPUT | NUM_ERROR | ACCUM_ERROR |
|---|---|---|---|---|
| 1 | 509-783-5167 | 509-783-5167 | 0 | 0 |
| 2 | SHARLENE CIRCELLI | SHARLENE CIRCELLI | 0 | 0 |
| 3 | 4018 W CLEARWATER AVE | 4018 W CLEARWATER AVE | 0 | 0 |
| 4 | KENNEWICK | KENNEWICK | 0 | 0 |
| 5 | BENTON | BENTON | 0 | 0 |
| 495 | GREENE | GREENE | 0 | 0 |
| 496 | PZ | PZ | 0 | 0 |
| 497 | 15370 | 15370 | 0 | 0 |
| 498 | 20/2/1927 | 20/2/1927 | 0 | 0 |
| 499 | FEMALE25 | FEMALE25 | 0 | 0 |
| 500 | ALPINE08 | ALPINE08 | 0 | 0 |

Hash Type = sha384 Percent error (%) = 0

INPUT: Input data from QR Code or expected output.
ACTUAL OUTPUT: Actual output after final verification.
ACCUM_ERROR: Number of accumulative errors between input and actual output.
PERCENT ERROR: [ACCUM_ERROR/COUNT] x 100%.

*Fig. 6 Report of Percentage of Error*

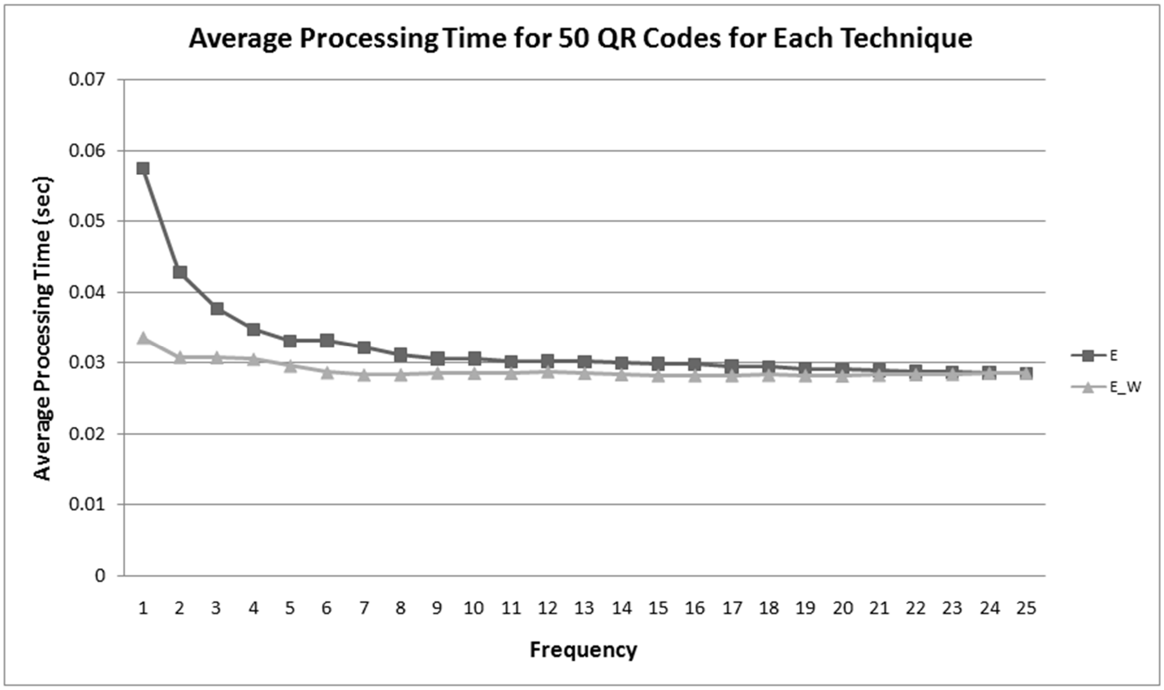


*Fig. 7 Graph of Average Processing Time for 50 MyID Cards (E = Existing Technique, E_W = Proposed Technique)*

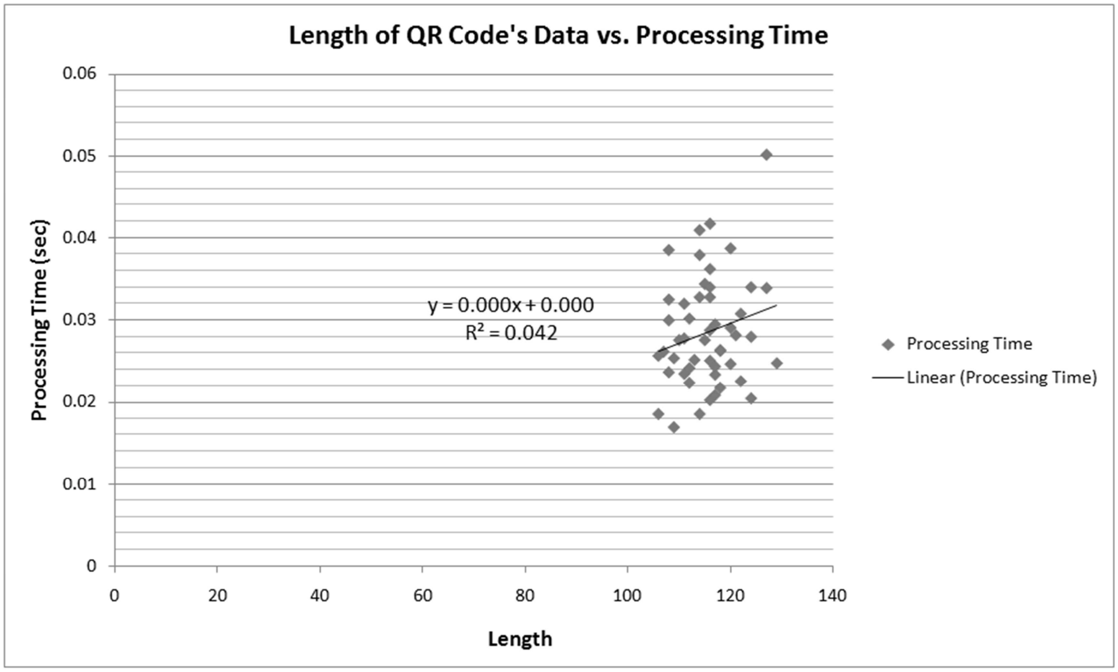


*Fig. 8 Graph of Processing Times for the Proposed Technique*