

ANNALS OF “DUNAREA DE JOS” UNIVERSITY OF GALATI  
MATHEMATICS, PHYSICS, THEORETICAL MECHANICS  
FASCICLE II, YEAR XII (XLIII) 2020, No. 2  
DOI: <https://doi.org/10.35219/ann-ugal-math-phys-mec.2020.2.03>

## A survey on applications for the hotel management system and tourists

George Petrea<sup>1</sup>, Ciprian Vlad<sup>1</sup>, Catalin Arama<sup>1</sup>, Marian Craciun<sup>1</sup>

<sup>1</sup> „Dunărea de Jos” University of Galati, Romania, e-mail: [ciprian.vlad@ugal.ro](mailto:ciprian.vlad@ugal.ro)

### Abstract

In the actual context of social distancing due to the Coronavirus, many hospitality facilities face an economic crisis. Tourists are very concerned and think twice before choosing to accommodate in a hotel. In order to limit human contact, many studies have been developed with the aim to find the best options for front desk services and tourist access control. Other issues that had to be taken care of were security and energy efficiency. This paper proposes a study of different hotel management facilities that should respond to the actual needs of both the hoteliers and the tourists, in order to ensure a safer and comfortable staying.

**Keywords:** hotel management system, acces control, QR codes, NFC.

### 1. INTRODUCTION

Tourism service providers are facing the biggest crisis in the last two decades, because of the new Covid 19. People choose now very wisely the places where they can spend their vacations and there are more and more demands for safe facilities and services. This is why hoteliers need to improve and to change their vision of tourism, in order to remain on the market.

On the other hand, service providers need to think about safety for their employees and to limit human contact with the tourist, to avoid the risk of infection with the new virus.

After all the safety issues, there is also the financial aspect that concerns the hoteliers. The new requirements in the actual context added new costs and restrictions and in order to be profitable, service providers are searching intensively for new and innovative solutions.

In the past, digital access control was based on the use of a personal identification number (PIN) that could be entered using a touchpad. The issues with this kind of system appear due to the possibility of forgetting the PIN or the risk of it getting into unauthorized hands. In the actual context, the touching of keypads is another issue because of the risk of infection.

Some contactless solutions have been implemented using radio frequency identification (RFID) systems. RFID technology is based on storing and remotely achieving data using RFID tags. The system uses radio waves for transmitting information from RFID tags to a host central computer [1], [2], [12], [13], [23].

Another way of having secure access to facilities is the use of biometric authentication systems. In this case, some unique physical part of tourists can be used as authentication keys. Fingerprints, face detection, iris detection, voice recognition are some of the proposed ideas. Nevertheless, some issues appear in the case of biometric systems, because of their complexity, implementation cost, the accuracy of identifying people, and hygiene problems [3],[4], [28].

Some of the innovative solutions implemented recently involve the use of robots as a front desk operator. The idea is studied in [5], [6], [7]. The issues with this kind of system could be the cost of such a solution and the capability of dealing with a large number of people at the same time.

Another idea recently developed is the use of Near Field Communication (NFC) systems. Actually, the development of smartphones and applications which offer vast and compelling storage

and computing capabilities changed the lifestyle of users. The next step was to integrate NFC into smartphones in order to open up more opportunities. The solutions first implemented required the storage and processing on a smartphone, thus there was the risk of attacks or phone getting in unauthorized hands [8], [24]. The next idea was that of using a secure digital key along with the NFC access system for enhancing the security of the access control system without additional hardware efforts. In [9] are proposed two additional authentication methods, one with a digital key on a NFC-enabled smartphone and one with Encrypted Steganography Graphical Password.

This paper makes a survey on the existing high-tech systems that can provide self-check-in capabilities using different techniques. QR codes, ESQR codes, and NFC applications are presented with different purposes while servicing tourists.

The rest of the paper is organized as follows. Section II discusses RFID systems. Section III presents some QR based systems that are used for servicing tourists in hiking or hotel booking and Section IV shows some applications based on NFC systems, also for hospitality. The last section will conclude the main results of the paper.

## 2. RFID TECHNOLOGY USED IN HOSPITALITY

The RFID technology refers to a system that uses radio signals for exchanging different data. The architecture (figure 1) of such a system is based on two components: a tag and a scanner.



*Fig. 1. Architecture of a RFID system [1]*

The scanner reads the information coded in the tag and, depending on the information received, takes action. Different actions can be executed, such as: number displaying, sending information to a point of sale (POS) device, etc. [14], [16]. The information is transmitted without contact between the tag and the scanner because the reader sends electromagnetic waves that form a magnetic field. In this way, the microchip's circuits of the tag are powered. The electromagnetic waves are modulated by the tag's chip and are sent back to the scanner that will convert the signal into digital data [23].

There are a lot of applications in which RFID is used, such as: POS, vehicle identification, animal identification, warehouse management, access control, etc.

For hospitality/tourism activities the applications that are suitable for RFID use are: payment in the hotel, keyless room entry, food, and beverage management [15].

## 3. QR CODE TECHNIQUES IN DIFFERENT APPLICATIONS

Nowadays Quick Response (QR) codes are largely used in applications in order to uptake relatively large amounts of data in a modern way. A QR code is a two-dimensional code that can be read faster than the classic barcodes and can give more information [17], [20], [25].

The initial intended use of QR codes was the identification of automobile parts for the manufacturing industry but now QR codes are also used in different applications such as: marketing promotions, supply chain management, etc.

The main advantage of a QR code is that it provides a secure, cheap, and easy way for transmitting information to different receivers, in a “push” format. The existing open source libraries that can be used for generating QR codes from different data sources represents another advantage. The amount of data transmitted depends on the revision version of the QR code, but at the reception, the programs/applications decrypt the message. [26], [30]. This facility gives the receiving application

the possibility to parse the data from the tag and use the information depending on how the programmer decides. Although each revision of codes has its own standards regarding availability, redundancy, or data integrity. As long as the QR code can be read, the codes will be used with any operating system as long as the open source encode/decode libraries are supported. Finally, another advantage of QR code using is the ensuring of data accuracy, because users cannot enter data manually.

In [10] the authors present the impact of QR codes used in combination with mobile services and web services for different government agencies. Two case studies are presented. The first application refers to National Park Services (NPS) which helps tourists that are visiting different national parks and the second one to Mobile Environmental System (MENVIS) which aims to support scientist and staff engineers to collect data from the field and also to enhance exploring, discovery experiences and learning for students or tourists while traveling in different urban environmental preservation areas.

The two platforms have the following features based on QR codes: the waypoint system – prevents tourists from getting lost. QR codes are added to trail markers and are used for helping tourists in navigating park trails; mapping data for Mobile Map Visualization- QR codes containing data about flora, fauna, trail route, etc. are used for visualization services for tourists; gamification-hiking activities can be integrated into gaming activities such as rewards seeking or scientific exploration; social media integration-tourists can share information about their activities on their social networks.

Figure 2 shows the architecture of the NPS system that provides information about maps, location, weather, rangers on duty, park status, etc. for tourists.

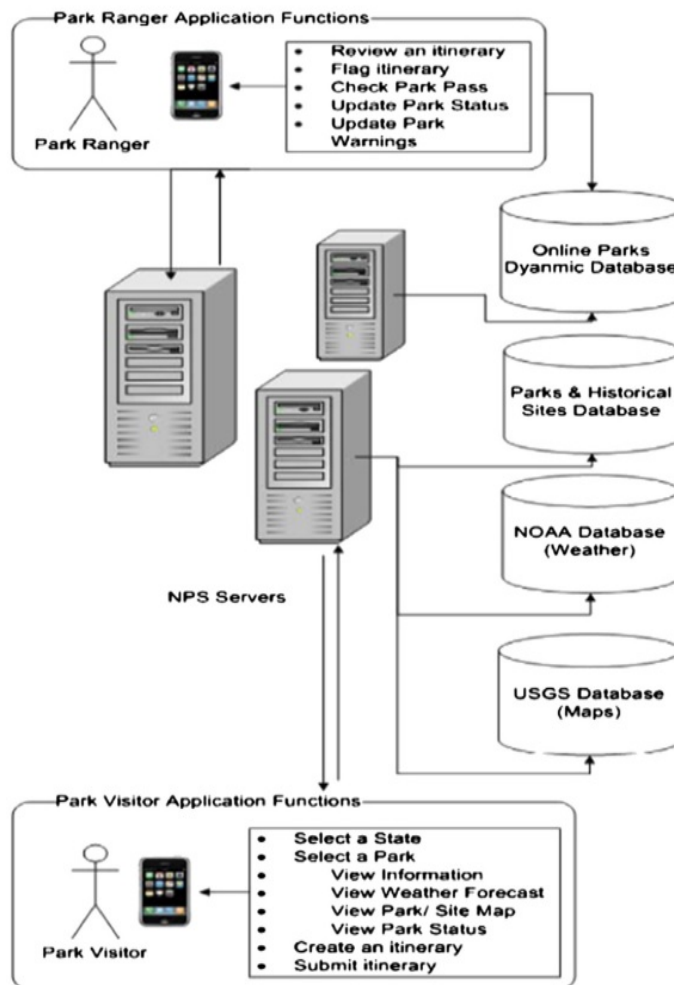


Fig. 2. QR code based NPS mobile service architecture [10]

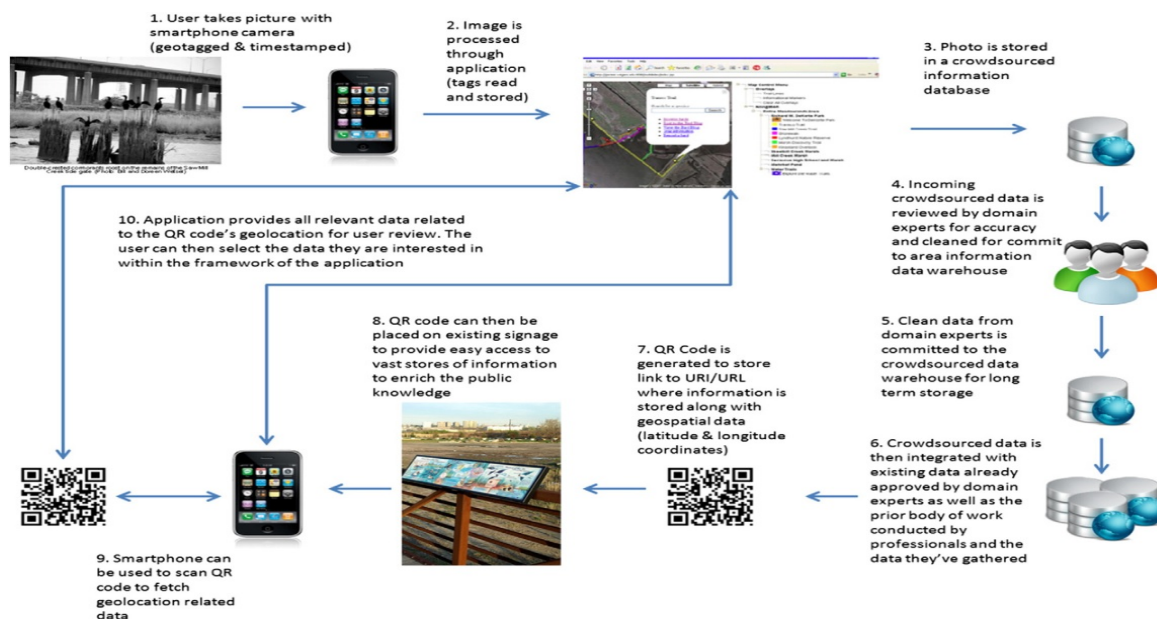


Fig. 3. QR code integrated into MENVIS system [10]

Figure 3 shows MENVIS’s process flow while using QR codes. This application has two operation modes: online and offline with different capabilities and features [27].

For the hospitality business in [11] is presented a unified hotel access control system (UHACS) which is used for booking and room access. UHACS is based on two subsystems, one for booking management and one for the door management system. Both subsystems used encrypted steganography quick access (ESQR) codes.

In the first subsystem, the booking procedure is managed, the system generates and checks the unique ESQR code for each tourist.

The second subsystem is composed of a control panel based on a Raspberry PI platform which is used for decoding the ESQR code and controls all the operations needed by the tourist using different modules: camera, network module, Bluetooth Low Energy (BLE) module, etc.

ESQR codes combine cryptography with steganography techniques in order to ensure enhanced security for the authentication process during check-in and for room access. UHACS is based on 6 main steps that are shown in figure 4. The first 3 steps are for the booking procedures and the last 3 steps are used to define the check-in and room access for guests.

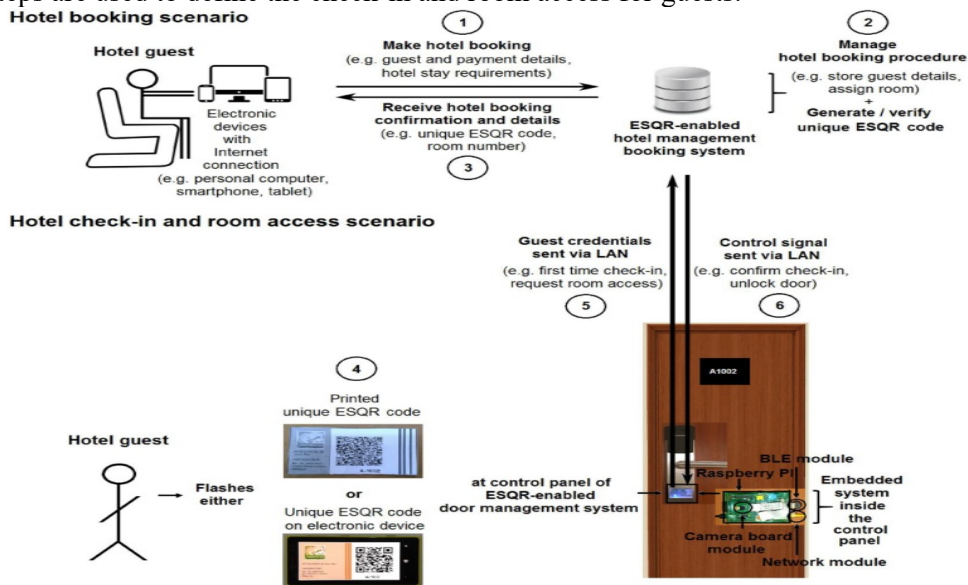


Fig. 4. UHACS for hotel management [11]

#### 4. NFC TECHNOLOGY USED IN HOSPITALITY

NFC is a new technology that is used for developing a lot of applications suitable for smartphone use. In the hospitality zone, some systems have been developed.

For example, in [9] is presented a NFC access control system using smartphones based on two credentials: one using a NFC-enabled smartphone with a digital key and another one with an Encrypted Steganography Graphical Password (ESGP) scheme. The goals of this system were to enhance the security of access control on one hand and to simplify the access, on the other hand, by offering the possibility to unlock doors using the NFC-enabled smartphone.

Figure 5 shows the NFC-ESGP registration process done with a digital key stored on a smartphone. The proposed solution has 3 base components: 1. A server for managing and registering clients using a computer/tablet (User Management Application); 2. A client application for supplying graphical password (Stego Acces Control-SAC); 3. A server for encoding/decoding the encrypted password (Middleware application).

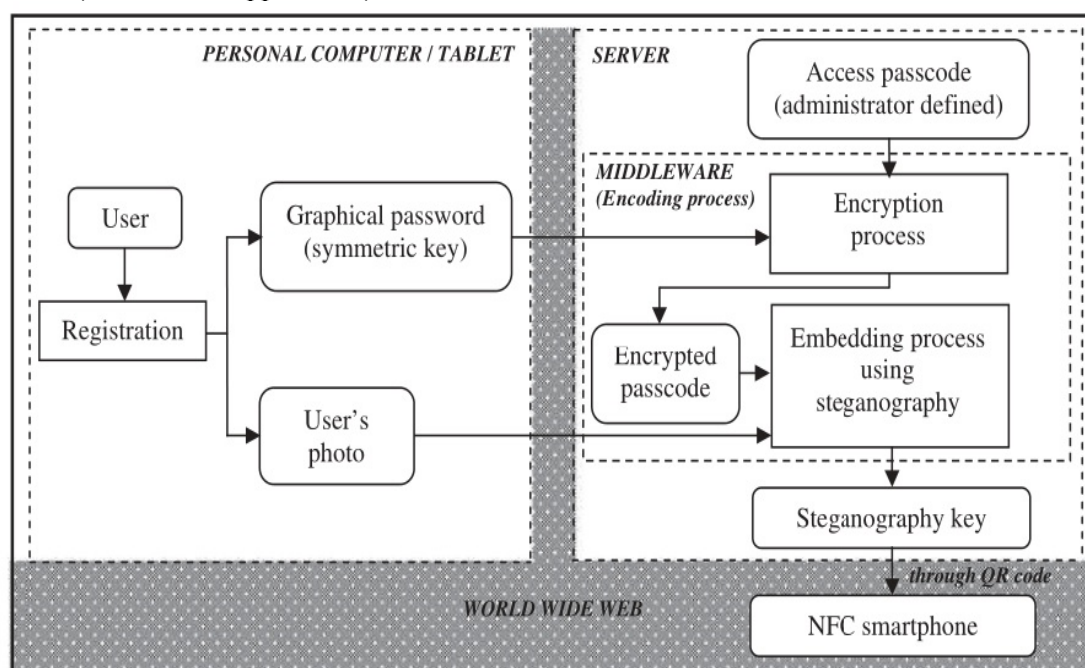


Fig. 5. NFC ESGP registration process [9]

The paper [9] details all the steps that are done for the registration process such as: steps for obtaining encrypted passcode, cryptography techniques used, and steganography technique used for obtaining the steganography key that is then transferred to users smartphone using QR code.

The first step for registration is to have a user photo like a self-portrait or representative object that will be used in a later stage for stego-photo generation [18], [19]. Next, the users choose three graphics from a 3x3 grid of graphics as a graphical passcode. This passcode is then used in an Advanced Encryption Standard (AES) cryptography technique with a key size of 256 bits. After this step, an encrypted passcode is obtained [21].

The next step is to embed the encrypted passcode into the host photo. In order to do that, the authors propose a steganography technique for obtaining a unique stego-photo for each user. The stego-photo will be used as a digital key. The steganography technique can be a spatial or transform domain technique and the authors use the LSB (least significant bit) spatial domain substitution [22], [29]. This transformation means that the LSB of each pixel from the host image is replaced with the embedded data until all data bits will be embedded into the pixels. By using this technique, the host image and the stego-image will preserve a high similarity. Also the LSB technique ensures a fast decoding process.



The steganography key obtained this way is the secure token that will be used by the server for user authentication. After the steganography key is obtained, the next step is to transfer it to the user's smartphone.

Finally, Figure 6 summarizes NFC-ESGP the decoding and verification processes done by SAC and Middleware. The first step for decoding is to extract the encrypted passcode using the same technique used in the encoding process. Next, the decrypted passcode is obtained and compared with the access passcode stored in the server. If the passcodes match, access is granted. The system implementation requires 5 components: a NFC enabled smartphone for running SAC application, a NFC reader to decode a launch NFC on a smartphone, a controller and stepper motor for door access, a server to host the User Management and Middleware applications, and a Wi-Fi LAN for communication between NFC smartphone and system.

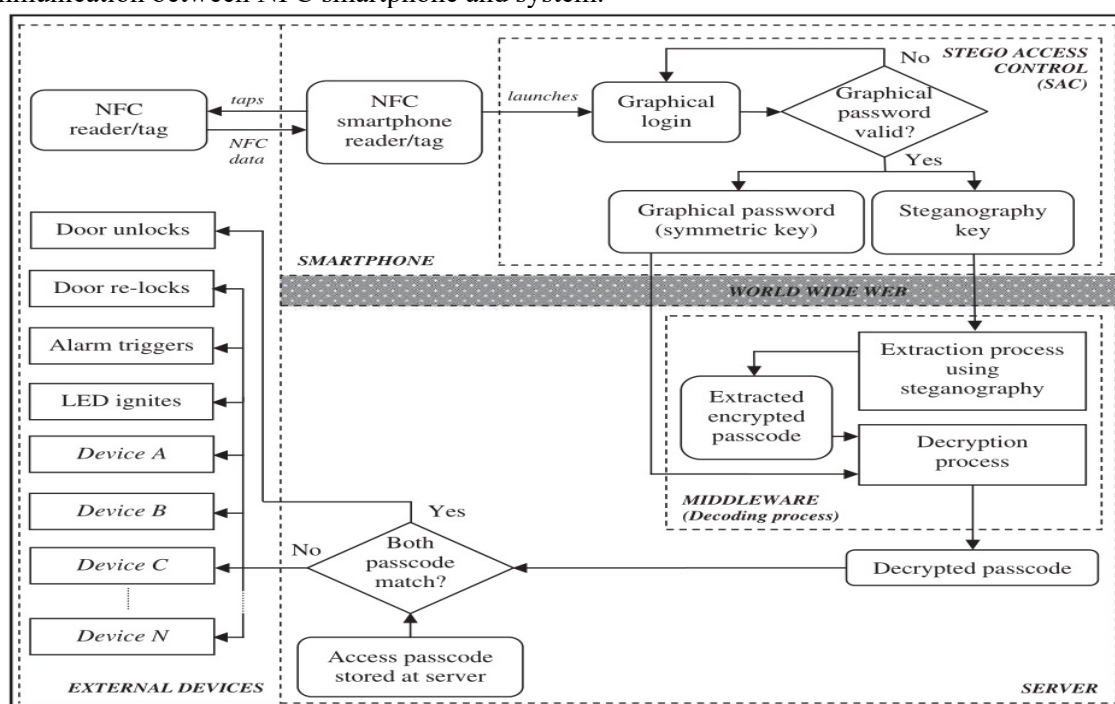


Fig. 6. NFC ESGP registration process [9]

## 5. CONCLUSIONS

Different systems and technologies were proposed in order to satisfy the needs of security and comfort for tourists. Now, with the appearance of Covid 19, everyone needs to keep a safe distance in order to prevent infection. This paper makes a survey on the existing applications and systems that can help both tourists and hotel management to keep the social distance. At the same time, the tourist needs to benefit from all the hotel services during his stay. There are also a lot of aspects during the stay at the hotel which should be taken care of, such as: climate control, food consumption, windows and lights control, which also involve energy saving issues. Although all existing technologies are based on microcontrollers, smartphones, sensors, and wireless transmissions, the applications are built to solve specific hotel/tourist issues, but a completely integrated HMS is not developed.

## References

1. Öztayşi B., Baysan S. Akpınar F., Radio frequency identification(RFID) in hospitality, Elsevier Technovation 29 (2009) 618–624.

2. Clarke R. H., Tewde D., Tazelaar J.R., Boyer K.K., Radiofrequency identification (RFID) performance: the effect of tag orientation and package contents., *Packaging Technology and Science* 19 (2006) 45–54.
3. Asha S., Chellappan C., Biometrics: An overview of the technology, issues and applications. *International Journal of Computer Applications*, 39(10) (2012) 35–52.
4. Zhang D., Guo Z., Lu G., Zhang L., Liu Y., Zuo W., Online joint palmprint and palmvein verification, *Expert Systems with Applications*, 38 (2011) 2621–2631.
5. Gockley R., Bruce A., Forlizzi J., Michalowski M., Mundell A., Rosenthal S., Sellner B., Simmons R., Snipes K., Schultz A., Wang J., Designing robots for long-term social interaction, *IEEE/RSJ international conference on intelligent robots and systems* (2005) 1338–1343.
6. Kanda T., Shiomi M., Miyashita Z., Ishiguro H., Hagita N., A communication robot in a shopping mall, *IEEE Trans. Robot* 26 (5) (2010) 897-913.
7. Pinillosa R., Marcosa S., Feliza R., Zalamab E., Gómez-García-Bermejjob J., Long-term assessment of a service robot in a hotel environment, *Robotics and Autonomous Systems* Volume 79 (2016) 40-57.
8. Clark M., GSMA staff get NFC hotel keys for mobile world Congress., <http://www.nfcworld.com/2013/02/26/322740/gsma-staffget-nfc-hotel-keys-for-mobile-world-congress/> (2013).
9. Cheong S.N., Ling H.C., Teh P.L., Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system, *Expert Systems with Applications* 41 (2014) 3561-3568.
10. Lorenzi D., Vaidya J., Chun S., Stafiq B., Atluri V., Enhancing the government service experience through QR codes on mobile platforms, *Government Information Quarterly* 31 (2014) 6-16.
11. Lim W.M., Teh P.L., Ahmed P.K., Cheong S. N., Ling H.K., Yap W.J., Going keyless for a seamless experience: Insights from a unified hotel access control system, *International Journal of Hospitality Management* 75 (2018) 105-115.
12. Juels A., Rivest R., Szydlo M., The blocker tag: selective blocking of RFID tags for consumer privacy, *Proceedings of the 10th ACM Conference on Computer and Communication Security*, Washington, DC, USA (2003) 103–111.
13. Blythe P., RFID for road tolling, road-use pricing and vehicle access control, *Proceedings of the IEEE Colloquium on RFID Technology* 123 (1999) 8/1–8/16.
14. Cerino A., Walsh W.P., Research and application of radio frequency identification (RFID) technology to enhance aviation security, *Proceeding of the IEEE 2000 National Aerospace and Electronics Conference* (2000) 127–135.
15. Fuschi D.L., Bo G., Saadia Y., Innovative applications for content distribution and consumption in tourism and education using PDA or mobiles, *Proceedings of the First International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution* (2005).
16. Hassan T., Chatterjee S., A taxonomy for RFID, *Proceedings of the 39<sup>th</sup> Annual Hawaii International Conference on System Sciences* (2006).
17. Bhuiyan M., Picking, R., A gesture controlled user interface for inclusive design and evaluation study of its usability, *Journal of Software Engineering and Applications* 4 (2011) 513–521.
18. Angeli A. D., Coventry L., Johnson G., Renaud K., Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems, *International Journal of Human-Computer Studies*, 63(1–2) (2005) 128–152.
19. Shejul A.A., Kulkarni U. L., A secure skin tone based steganography using wavelet transform, *International Journal of Computer Theory and Engineering* 3(1) (2011) 1793–8201.
20. Suo X., Zhu Y., Owen G.S., Graphical passwords: A survey, *Proceedings of the 21st Annual Computer Security Applications Conference* (2005) 463–472.

21. Ferguson N., Schneier B., Kohno T., *Cryptography engineering: Design principles and practical applications* (1st ed.), Indiana, USA: John Wiley and Sons, 2010.
22. Goel S., Rana A., Kaur M., Comparison of image steganography techniques, *International Journal of Computers and Distributed Systems* 3(1), (2013) 20–30.
23. Meena N., Ahmed J., Mujahid U., RFID system: Design parameters and security issues, *World Applied Sciences Journal* 23(2) (2013) 236–244.
24. Raza M., Iqbal M., Sharif M., Haider, W., A survey of password attacks and comparative analysis on methods for secure authentication, *World Applied Sciences Journal* 19(4) (2012) 439–444.
25. Kan T.W., Teng C.H., Chou, W.S., Applying QR code in augmented reality applications, *Proceedings of the 8th International Conference on Virtual Reality Continuum and its Applications in Industry, VRCAI'09* (2009) 253–257.
26. Kieseberg P., Leithner M., Mulazzani M., Munroe L., Schrittwieser S., Sinha M., et al., QR code security, *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, MoMM'10* (2010) 430–435.
27. Chun S.A., Adam N.R., Atluri V., MENVIS: Mobile environmental information system, *Proceedings of the 8th annual International Conference on Digital Government Research: Bridging Disciplines & Domains (DG.O '07)* (2007) 286–287.
28. Jain A.K., Ross A., Prabhakar S., An introduction to biometric recognition, *IEEE Transactions on Circuits and Systems for Video Technology* 14(1) (2004) 4–20.
29. Katzenbeisser S., Petitcolas F.A., *Information hiding techniques for steganography and digital watermarking*, Norwood, Massachusetts, USA: Artech House, 2000.
30. Semmangaiselvi K., Vamsidhar T., Chandana K.H., Priya B. K., Nalina, E. An effective secure environment using graphical password authentication scheme, *International Journal of Engineering and Computer Science* 2 (2013) 383–490.