Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210290

Highly Secured Dynamic Color QR Pattern Generation for Real Time Application

R.Sanjjey [a,1], S.Abisheak [a], T.R.Dineshkumar [a], M.Kirthan [a], S.Sivasaravanababu[a]
[a] *Department of Electronics and Communication Engineering, Vel Tech High Tech Dr Rangarajan Dr Sakunthala Engineering College, Chennai, TN, India*

Abstract. This work advances the state-of-art secured WBAN system and QR pattern enabled authentication for privacy measures. An attempt was made to integrate all the above process to build high performance WBAN system. In this work, a comprehensive statistical framework is developed with randomized key generation and secured cipher transformation for secured sensor node communication. We create primary colour channels based on three different QR codes that are widely used for colour printing and complementary channels for capturing colour images. Last but not least, we produced a colour QR pattern.

Keywords. WBAN system, primary colour channels, QR codes

1. Introduction

The security measures inadequacies inherent in WBAN systems have driven the development of a new security model. On the other end applications of wireless sensor networks have been emerged steadily, ranging from industrial management to healthcare applications which leads key management and distribution poses significant challenges, especially in resource constrained sensor networks. When it comes to wireless communication using sensor nodes security measures plays a vital role for reliable communication which has to be addressed [1]. Thus, Security is one of the essential things needs to be incorporated and challenging task needs to be accomplished with traditional cryptographic algorithms due to following reasons: i) Typical sensor nodes consist of a tiny computing device that forward information to the destination node. ii) Memory, energy and bandwidth constraints. iii) Demands high throughput rate. Conventional block ciphers are not optimal for sensor networks due to its computation and hardware complexity overhead. The primary concern over many existing binary sequences extraction process for biometric key extraction is that they are complex in nature and poor resource efficiency which is incompatible with sensor networks. In recent years, ECG signal models have gained momentum in security applications for low complexity and complete randomness [2].

[1] *R.Sanjjey,* Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai. India; E-mail: sannjeyravichandran@gmail.com.

Though key generation from ECG signals are optimal for sensor networks since it doesn't require pseudo-random number generators (PRNG) and memory for seed storage it has the least invariance level over time period and significantly correlate with other classes which will affect uniqueness properties.

2. Specific Objectives

- To develop a novel tiny encryption modeling for secured sensor data communication.
- To develop QR pattern generation using color selection key to incorporate authentication requirement from WBAN applications.
- To develop key based QR pattern driven data protection and access control for WBAN system.
- To develop cloud storage mechanism for WBAN technology and security and privacy of patient and medical personals.
- To perform hierarchical complete processing steps involves in real time WBAN health care system.

3. Proposed System

The inadequacies inherent in existing WBAN system have driven the development of new light weight hardware architecture and to exploit the benefits of biometric characteristics of ECG biomedical signal for key generation task in digital crypto systems for high performance security system filter [3]. Moreover, FPGA devices have been used extensively for high throughput applications but they cannot full fill the several Gbps throughput requirement of next generation systems, and low power consumption with the invention of power compatible 5G devices. Such systems rely fully on arithmetic techniques used to carry out computation. In general bio cryptosystem framework includes a number of benefits: i) it uses the random binary sequence generated from input biometric, which solves key management issues with low computational cost. Most of the existing key generation methodologies are not completely random in nature to transform the input sequences into cipher and computationally intensive in nature. ii) the proposed bio-cryptosystem generate different binary sequences for every class and thus preserves discrimination; iii) this scheme is secured and more efficient as compared to other block Cipher; iv) completely randomized transformation nature of proposed bio-cryptosystems suits for both text and image encryption. This work is guided by the motivation of extending the merits of light weight crypto model to improve the performance of diffusion and confusion computations since highly simplified arithmetic computations only involved in light weight crypto system. This thesis is focused on the cipher key generation using ECG signal to deal with the challenging key management problems.

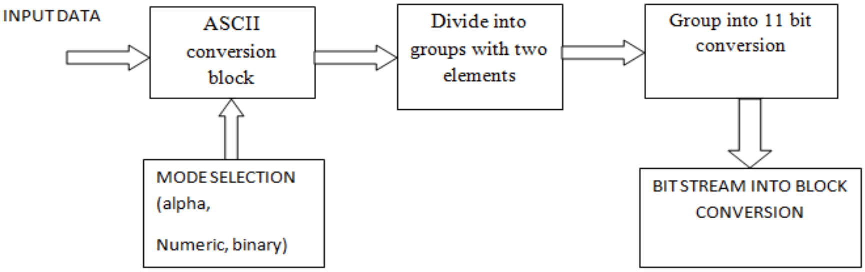

INPUT DATA
ASCII conversion block
Divide into groups with two elements
Group into 11 bit conversion
MODE SELECTION (alpha, Numeric, binary)
BIT STREAM INTO BLOCK CONVERSION

Figure 1. Bit stream to Block Conversion

4. Access Control Model

Authenticity in WBAN denotes the medical information transfer from access point to the storage space and rule sets to define each valid group. The basic parameters required for reliable medical data communication in WBAN and associated security measures are as follows:

Data authenticity: In multi path data propagation during wireless data communication some intended attacks are carry out using malicious nodes which is called bogus sensor; thus, the end terminals should validate the sensor nodes origin of information to ensure the data authenticity

Data confidentiality: The WBAN system is highly vulnerable to all kinds of passive attacks due to its open access nature and allows some loophole to reveal all personal information's about patient to external users. It is essential to overcome this limitation using crypto core based secured biomedical data transmission in all phases. Data integrity: To handle this WBAN system should verify the sensor details during data integration. Data availability: It comes under denial-of-service (Dos) related attacks over medical server where sensor information's are collected and stored. In case of access denials during medical services causes complete WBAN system failure. In most cases some unique detection methodologies are incorporated to detect the avoid this DOS attacks. IN order to narrow down the human intervention in automated patient monitoring system without compromising the reliability several hierarchical transformations are introduced between end-to-end data communication which starts from data collection using body sensor to the cloud database. It also includes data authentication and accessibility by medical personals. Here the proposed WBAN system includes some novel approaches in both access control and data security. Here some unique key driven QR pattern generation and associated color selection of each generated patterns all potential attacks are prevented.

4.1 Color variant QR pattern for authentication

Due to its inherent error correction mechanism and associated data embedding metrics, QR patterns have been widely motivated for authenticating several commercial commodities including cloud data. It makes use of simplest computational process during QR code generation which allows better readability to all available QR code readers in smart phones. In particular unique color selection for each patterns allows them to accommodate several million users in this proposed WBAN healthcare system. Here sensor nodes are authenticated at the server side using QR pattern.

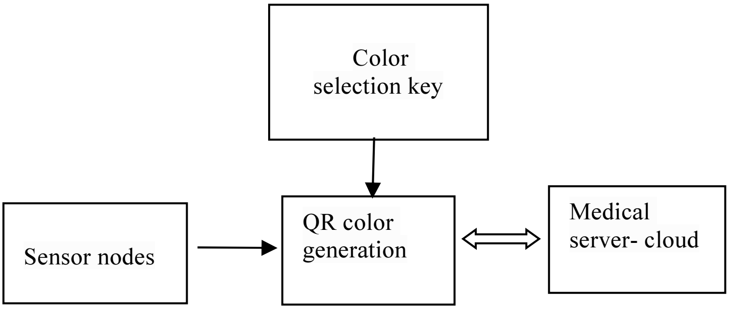


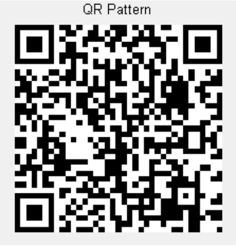
Figure 2. QR pattern authentication

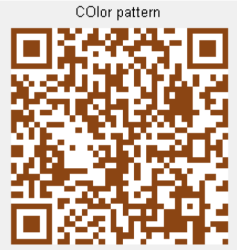
QR pattern variants are used to manage WBAN access and protect data. Patients are recorded in cloud storage using a colour key created from their patient ID to convert their personal information into a QR pattern. During data transmission to the cloud, the sensor information from access points must be validated. The level of protection and resistance to malicious attacks is determined by colour variants. Color key randomization enhances major confusion metrics, and QR patterns' inherent error correction capabilities allow for the lowest possible false detection rate during validation.. Moreover, all these QR patterns are generated from some unique user defined details or template data and this QR pattern generation-based data authentication doesn't altered the original data since it makes use some mapping function or one way transformation.

5. Summary

The first part of this chapter discusses the proposed WBAN system's goals. The second section delves into the security methodologies employed in the efficient processing of WBAN data, followed by a thorough explanation of the characteristics. This work focused on the generation of color QR pattern for WBAN system cloud integration. In addition to that this chapter discussed in detailed about the performance metrics of WBAN system with the inclusion of QR pattern analyzes. The proposed methods show the adequate performance when compared to the existing methods.

6. Results and Conclusion





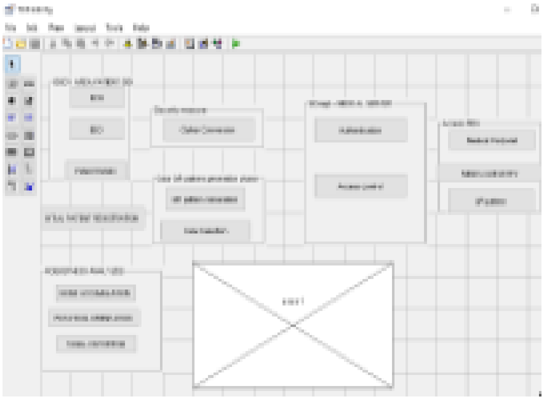
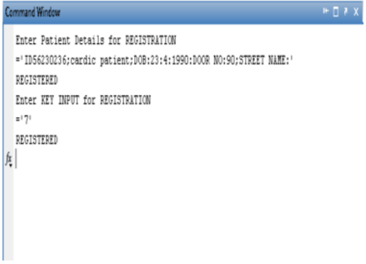
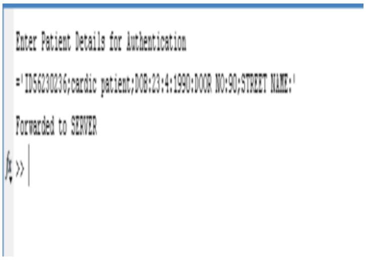


Figure 3. Input GUI Model

Here push buttons were created along with axes plot for dynamic user inputs and associated relevant results for each input dynamics. Both authentication and access control mechanism can be easily validated.



```
Enter Patient Details for REGISTRATION
='ID56230236;cardic patient;DOB:23:4:1990:DOOR NO:90;STREET NAME:'
REGISTERED
Enter KEY INPUT for REGISTRATION
='7'
REGISTERED
fx |
```



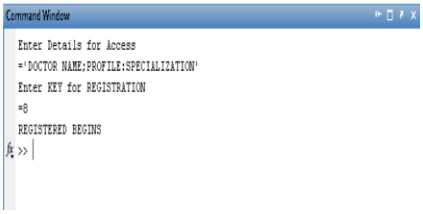
```
Enter Patient Details for Authentication
='ID56230236;cardic patient;DOB:23:4:1990:DOOR NO:90;STREET NAME:'
Forwarded to SERVER
fx >> |
```

Figure 4.a. Patient details and generated QR pattern **Figure 4.b.** Input Patient details server updation

After obtaining the user details from different individuals color QR codes are generated based on selected key components and forwarded it to medical server as a core template. With this method, instead of predetermining the user data as statistical values QR patterns are generated for all given inputs and construct as single compound templates which has all the basic properties of cancelable template.

6.1 Data authentication output

After obtaining the user details from different individuals color QR codes are generated based on selected key components and forwarded it to medical server as a core template. With this method, instead of predetermining the user data as statistical values QR patterns are generated for all given inputs and construct as single compound templates which has all the basic properties of cancelable template.



```
Enter Details for Access
='DOCTOR NAME;PROFILE:SPECIALIZATION'
Enter KEY for REGISTRATION
=8
REGISTERED BEGINS
>>
```

Figure 5.a. Access control model output

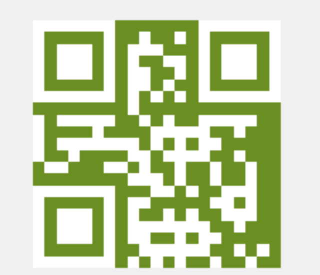


Figure 5.b. Modified QR pattern

6.2 Color key driven data authentication

The randomization of component key and pattern selection provides major benefits. Non-inevitability steps I QR patterns' built-in error correction metrics minimise false detection rates during validation (ii) due to compound template generation, variance in input trails won't be tolerated during validation because each template contains fine information from various types of multi modal system

7. Conclusion

Here we analysed the performance of color and pattern selection QR image for WBAN based applications of secured data transfer, data authentication and privacy measures. We also introduce the idea of toned – noisy – Rotated colour QR images, as well as a method for automatically decoding these QR codes. The graceful potential metrics of the QR pattern and its perceptual quality as a feature of embedding parameters in WBAN applications are demonstrated experimentally.

References

[1] Zhang, C., Wang, J., Han, S., Yi, M., & Zhang, Z. (2006). Automatic Real-Time Barcode Localization in Complex Scenes. 2006 International Conference on Image Processing, 497–500. https://doi.org/10.1109/ICIP.2006.312435

[2] Yang, H., Jiang, X., & Kot, A. C. (2010). Accurate localization of four extreme corners for barcode images captured by mobile phones. 2010 IEEE International Conference on Image Processing, 3897–3900. https://doi.org/10.1109/ICIP.2010.5651603

[3] Huijuan Yang, Kot, A. C., & Xudong Jiang. (2012). Binarization of Low-Quality Barcode Images Captured by Mobile Phones Using Local Window of Adaptive Location and Size. IEEE Transactions on Image Processing, 21(1), 418–425. https://doi.org/10.1109/TIP.2011.2155074