World Applied Sciences Journal 29 (9): 1170-1174, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.09.1432

Authentication Verification and Remote Digital Signing Based on Embedded Arm (LPC2378) Platform

B. Karthik and T.V.U. Kiran Kumar

Department, Bharath University, No: 173, Agaram Road, Selaiyur, Chennai-73, India

Abstract: In the current digital world, the need for digital signing has increased exponentially. Generally, any electronic documents transmitted electronically or physically needs to verified whether it was tampered or not, technically digital verification/authentication. Digital signing is one of the digital frameworks that could effectively address these issues in an optimized basis. In brief the project can be explained as; we get an analog or digital data that will be given as an input to DSP executable chip (via A/D interface) which performs basic image operations. The processed data would flow through a 32-bit embedded ARM microprocessor and the processor (that performs digital encryption via RSA or IDEA algorithm) and outputs an encrypted solution. By using this system we could be able to transmit the data of preferred length based on the user or application requirement. Further, the digitally encrypted data can be transmitted via Ethernet. The Ethernet incorporated in this system offers dual redundant network and long distance communication function, which can ensure the disturb rejection capability and reliability of the communication network.

Key words: Digital signing · LPC2378 · SHA256 · Two dimensional barcode · Octave and keilUvision4

INTRODUCTION

Barcode is an optical machine readable representation of data which provides essential information regarding products over which they are imprinted. The information (i.e. price, mgf date, exp date and unique lot number and product number) of any product could be represented via width of the lines and the spacing provided between the lines (black and white lines). Further, barcodes allows the user to collect the data in real time consistently, accurately and rapidly [1]. The barcodes are generally read via optical scanners (barcode readers), image acquisition tool box or scanned from an image by special software.

The art of mapping the data to barcode is known as symbology. In this framework, we transform the data into binary stream that was encoded via single digit or character of the message into bars and spaces. Based on the encoding process, barcodes are classified into two types: namely linear (1D) barcodes and matrix (2D) barcodes.

The basic drawback of one-dimensional barcodes is lower data representation capability that has now grown as major concern as the amount data needed to imprint has increased drastically [2]. On the other hand, two-dimensional barcodes have more data representation capability and contain more detailed information. They can be in matrix or stacked format. The 2D barcodes can able to store large amount of data, these can able to store up to thousand of alphanumeric data [3, 4]. These can able to store data in both horizontal and vertical direction. It is possible to retrieve the lost data in 2D barcodes as these barcodes will contain the error correction capabilities, which allows the data to be retrieved even after barcode label is damaged.

A certificate (license) is an official written or printed statement that may be used as proof or evidence of certain facts. So far all kinds of soft certificates can be very easily forged, juggled and embezzled, which greatly weakens their authority and credit system. Obviously this fact poses a growing threat to the social order and has become a critical problem. Therefore,

Corresponding Author: B. Karthik, Department, Bharath University, No: 173, Agaram Road, Selaiyur, Chennai-73, India.

several organizations are looking for the new anti-counterfeit techniques used to protect the information in soft certificates has been increasing exponentially [5]. Several applications have been designed that could offer information security such as authentication, data integrity and non-repudiation of certificate (license).

A digital signature is a framework that generates a signature component using a hash of an encrypted/unencrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message. Hence, digital signature is a term used to describe a data string which associates a digital message with an assigned person only.

A hash function is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array (cf. associative array) [6]. The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes. A minute alteration in data would deliver a digest with a greater difference between the delivered hash digest to original stored digest. It is easy to compute the hash value for any given message. It is not possible to know the content message for the given hash functions. It is also used in many encryption algorithms. Hash functions are mostly used to speed up table lookup or data comparison tasks such as finding items in a database, detecting duplicated or similar records in a large file and finding similar stretches in DNA sequences. In this system SHA-256 hashing is used which produce a 64 bit will hash value for data that which is given as input.

Octave is a high-level language, primarily intended for numerical computations [7]. It provides a convenient command line interface for solving linear and nonlinear problems numerically and for performing other numerical experiments using a language that is mostly compatible with MATLAB. It may also be used as a batch-oriented language. The Octave language is an interpreted programming language [8]. It is a structured programming language (similar to C) and supports many common C standard library functions and also certain UNIX system calls and functions. However, it does not support passing arguments by reference.

The rest of the paper is organized as follows. First, in the next section, we briefly discuss the general design criteria for two dimensional barcode. Next, in Section 3, we describe the proposed system and discuss its advantages. Finally, we present some performance results in Section 4 and give our conclusions in Section 5.

2D Barcode Designcriteria: Hence, we designed a framework of digital signing of digital and electronic documents via imprinting barcode based on the hash code. Although barcode was invented about sixty years ago, barcode technology became applicable for value-added services in telecommunication industry just few years back [9]. Nevertheless, some issues regarding reliability, security and performance still exist and therefore digital signing for remote authentication lifecycle has to be analyzed carefully in order to be adopted and implemented into a given system**.**

The 2D barcodes proposed in the earlier section are more sophisticated standards that exist in the digital market. These are based on two dimensional symbologies, i.e. data would be encoded along the vertical and horizontal directions as well. Ordinary barcodes (1d barcodes) are vertically redundant, meaning that the same information is repeated vertically [10]. The heights of the bars can thus be truncated without any information loss. However, the vertical redundancy allows a symbol with printing defects, such as spots or voids to still be read. The higher the bars are, bigger is the probability that at least one path (horizontal section along the barcode) is still readable. A two dimensional (2-D) code stores information along the height as well as the length of the symbol (in fact, all human alphabets are 2-D codes).

Due to need of higher capacity and necessity of additional features, we are focusing on employing 2-D barcodes for Digital signing framework in this project.

In the section, we present a simplest 2-D barcode for remote signing purpose of the digital information. We considered QR barcode as the basis of designing the currently barcode and it would include the follows:

Finder Pattern: It is used for detecting the position of the barcode. By arranging this at the three corners of a symbol, the position, the size and the angle of the symbol can be detected (0 - 360°).

Alignment Pattern: This is used for correcting the distortion of the proposed barcode. It is highly effective for correcting nonlinear distortions.

Timing Pattern: It is used for correcting the central coordinate of the data cell in both vertical and horizontal directions.

Data Area: The barcode would store data in the data area. The data will be encoded into the binary numbers of '0' and '1' based on the encoding rule.

Symbol Size: The size of the barcode can be selected according to the data volume to be stored and the reading method (max: 43x43 based on the given hardware capabilities).

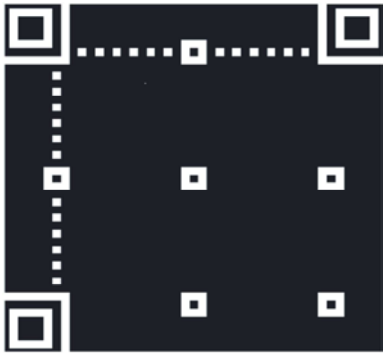

Fig.ure: Basic structure of proposed 2D-barcode

Proposed System: This paper mainly deals with the authentication of the electronic document. The authentication of a document is verified by following manner. Initially we should calculate the hash value of the data and this hash value is to be placed in a 2D barcode which is designed as discussed in section 2.

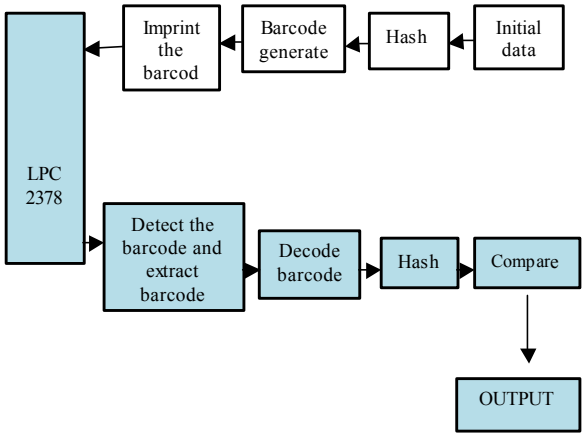

Figure: proposed system architecture

whenever we need to verify the authentication of the document the barcode is processed to LPC 2378 board where it will decode the barcode and the data present in the barcode is extracted and this data is compared with the data present in the SD card which is connected to the LPC2378 board and if the data is said to be found in SD card than the document is said to be authenticated.

Generate a two dimensional barcode with finder pattern, alignment pattern and timing pattern as specified in the section 2. Now place the data that is to be encoded on barcode into a text file and open the file in read mode and convert the data present in the file into 8 bit binary form[11]. After encoding the barcode with the data on to barcode imprint the barcode where ever it is necessary and this imprinted barcode will be given as input to the lpc2378 board.

Barcode authentication can be verified in two different scenarios. This is discussed in brief below.

In the first scenario firstly the digital document is encrypted and its hash value is calculated and the hash value of the encrypted data will be encoded into the barcode and that would be imprinted. And the imprinted barcode would be given as an input to the LPC2378 board upon successful image acquisition and the barcode would be extracted from the image that is given as the input to the board and the extracted barcode is decoded in order to get the information present in the barcode and this data is compared with the encrypted and hashed data associated with the original digital if the comparison is successful than it is said to be verified that the original digital document is un modified and it integrity is unaltered.

In the second scenario firstly we will calculate the hash value of the digital document and this hash value will be encoded on to the barcode and this barcode is imprinted. It is given to the LPC2378 board and this will firstly extract the barcode from the image that has been taken as the input and this extracted barcode is decoded to get the actual data present in the barcode once the barcode is decoded its content is saved into a file. As we will be having the authenticated digital documents hash values already in the SD card of the LPC2378 now search whether the content that is saved in the file is present or not in the external memory of the board if it is found than the digital document is said to be authenticated else it is said to be not.

Presently now in this paper second scenario is being implemented.

This can be implemented for remote access, access into an organization, electronic document authentication verification, mobile valet, Ecommerce, secure access and so on.

RESULTS

In this project the results are carried out by using the following LPC2378 microcontroller and the octave software, serial interface connected to the pc and the ulink2 debugger. In the below show figure firstly the data is placed in the barcode and then the barcode is incorporated in the card and then the barcode is extracted whenever we need to verify the authentication and the hash value of the data present in the barcode is calculated and used for verification of the authenticity of the card. Consider the below show figure how the authenticity is verified for access into an organization.

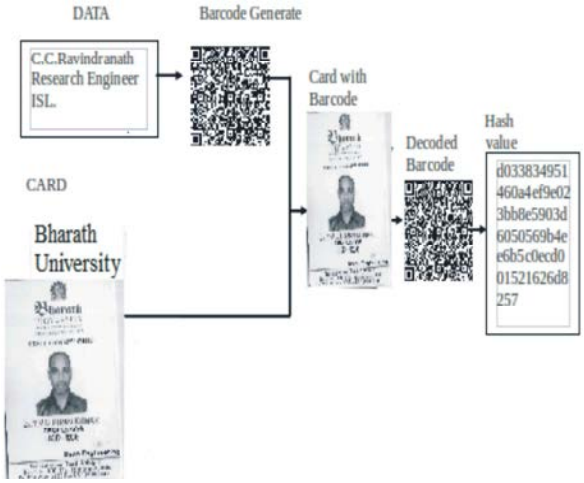

Figure: Shows how the entire project work goes

Test Simulation Checking the Authenticity of the Card with Respect to the Organization: For testing this case, we would consider 6 cards that are issued by the organization and of those two cards are expelled (due to various reasons) from the organization and these cards information has been removed from the database when ever if these cards try to access they should not be allowed. For example, Card 1, 2, 4 and 6 are presently related to the organization and card 3 and 5 are no longer related to the organization and the information regarding to this cards have been removed from the data base when ever if some tries to access with card 3 or 5 it will deny their access with the cards which are no longer related to the organization [11].

CARD 1 CARD 2 CARD 3

CARD 4 CARD 5 CARD 6

CARD	AUTHANTICATED	NOT AUTHANTICATED
Card1	Yes	
Card2	Yes	
Card3		Yes
Card4	Yes	
Card5		Yes
Card6	Yes	

Test simulation addressing the computational time with respect to remote authentication:

Time taken for incorporation of data on to card and to extract the barcode from card are tabulated below

CARD	Incorporate data(in sec)	Extract barcode(in sec)
Card1	3.90625	2.45312
Card2	3.12500	1.73480
Card3	8.53125	3.46875
Card4	5.03125	1.73438
Card5	5.39062	1.82812
Card6	5.53125	3.04688

The average time taken by the hard ware to verify the authenticity is approximately 45 seconds

CONCLUSIONS

We have successfully integrated the advantages associated with 2-D barcode and digital signing to effectively address these issues of remote authentication and verification. The basic model associated with remote verification framework was demonstrated in this project and the simulation results show that it has answered all the issues pertaining remote verification applications.

Further, the digitally encrypted data (i.e. hash code) will be transmitted via USB interface. This could be easily extended to other transmission interfaces, which ensures the disturb rejection capability and reliability of the communication network. The proposed system drastically reduced the computation time as it uses the secured hash codes for the comparison purpose. This system also preserves the identity of the individual role in the organization as the data is converted and stored via barcodes over the card [12-14].

In future work, we are planning to address the reduplication of the rejected cards or current assessable cards for malicious activities. This enhancement would make the proposed easily applicable for secured access in an organization.

REFERENCES

1. ISO/IEC 18004: ISO Standard on QR Code 2005 Bar Code Symbology Specification.
2. 2D Code and Barcode Image Generator: Denso Wave Incorporated, Japan.
3. http://www.nxp.com
4. Tool kit for bar code recognition and resolving on camera phones-jump starting the internet of things: Robert Adelmann, Marc Langheinrich, Christian Florkemeier institute for pervasive computing, ETH Zurich
5. http://en.wikipedia.org/wiki/Digital_signature
6. www.hitex.co.uk
7. Tabuman, D. and M. Marcellin, 2002. JPEG2000: Image Compression Fundamentals, Standards and Parctice. Norwell, MA: Kluwer.
8. Sundarraj, M., 2013. Study Of Compact Ventilator, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 16(12): 1741-1743.
9. Sundar Raj, M., T. Saravanan and R. Udayakumar, 2013. Energy Conservation Protocol for Real time traffic in wireless sensor networks, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1822-1829.
10. Sundar Raj, M. and T.R. Vasuki, 2013. Automated Anesthesia Controlling System, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 15(12): 1719-1723.
11. Sundar Raj, M., T. Saravanan and R. Udayakumar, 2013. Data Acquisition System based on CAN bus and ARM, Middle-East Journal of Scientific Research, ISSN: 1990-9233, 15(12): 1857-1860.
12. Abou-Deif, M.H., M.A. Rashed, M.A.A. Sallam, E.A.H. Mostafa and W.A. Ramadan, 2013. Characterization of Twenty Wheat Varieties by ISSR Markers, Middle-East Journal of Scientific Research, 15(2): 168-175.
13. Kabiru Jinjiri Ringim, 2013. Understanding of Account Holder in Conventional Bank Toward Islamic Banking Products, Middle-East Journal of Scientific Research, 15(2): 176-183.
14. Muhammad Azam, Sallahuddin Hassan and Khairuzzaman, 2013. Corruption, Workers Remittances, Fdi and Economic Growth in Five South and South East Asian Countries. A Panel Data Approach Middle-East Journal of Scientific Research, 15 (2): 184-190.