An Implementation of a Paper Based Authentication Using HC2D Barcode and Digital Signature

Puchong Subpratatsavee, Pramote Kuacharoen

An Implementation of a Paper Based Authentication Using HC2D Barcode and Digital Signature

Puchong Subpratatsavee[1] and Pramote Kuacharoen[2]

Department of Computer Science, Faculty of Science at Siracha
Kasetsart University Siracha Campus
199 Sukumvit Rd. Siracha, Chonburi 20230 Thailand
Department of Computer Science, Graduate School of Applied Statistics
National Institute of Development Administration
118 Serithai Rd. Bangkapi, Bangkok 10240 Thailand
puchong.sp@gmail.com[1], pramote@as.nida.ac.th[2]

Abstract. Paper-based documents are important and still widely used in government agencies and private entities as some documents cannot be replaced by electronic documents. These include loan agreements, dispatch or contracts, household registrations and passports. They must be paper-based. Paper-based documents can be easily forged with a printer and a scanner, and imaging software can easily edit them. This paper presents a paper-based document authentication by applying a digital signature and HC2D barcode to verify the integrity of the text message and the sender of the document. This is useful both for a quick inspection of documents with large quantities and monitoring that may help prevent fraud and forgery which may have occurred.

Keywords: HC2D barcode, paper-based document, digital signature, authentication

1 Introduction

The documents in a paper format are still important and still widely used in organizations or for personal proposes because some documents cannot be replaced by an electronic document. Examples are loan agreements, driver licenses, passports, etc. [1]. These documents are often forged and easily modified by criminals. The forged documents in the form of paper can be accomplished by using a printer and a scanner, and imaging software. The devices are relatively inexpensive and easily obtained and the image software can be used to edit the documents. Therefore, it is difficult to prevent the forgery from fraudster [2]. Although there are attempts to prevent forgery by putting chemicals or watermarks on the documents, it makes monitoring more difficult because some types of the protected documents require an expert for monitoring and inspecting. Consequently, this can take a significant amount of time.

This paper presents the process of authentication of text on a paper-based document by applying a digital signature and a 2D barcode, specifically, HC2D barcode.

Using this method, text on a paper-based document can be authenticated. This can verify the document author if the document has not been tampered with and can detect whether or not the document has been altered by an unauthorized person. The paper based document can be verified without the need of special equipment or expertise. Moreover, this method is very convenient and inexpensive.

2 Background and Related Work

This section provides background information and related work.

2.1 2D Barcodes

2D barcodes [3] are geometric patterns in two dimensions. The two-dimension barcodes have more data capacity than one-dimensional barcodes while using a smaller space because they can store data in both vertical pixel and horizontal pixel directions to support a large information distribution and detection without accessing the database or any storage tools. Generally, 2D barcodes contain black square pixels on a white color background. Currently, the 2D barcodes that are common are QR Code [4][5], PDF417 barcode [6], Maxi Code, Aztec Code [7], and Data Matrix [8] [9]. However, HC2D barcode [10] has a higher capacity. The characteristics and properties of the 2D barcodes are show in Table 1.

A HC2D barcode is a 2D barcode, which consists of a black square pattern on white background. The HC2D barcode contains information in the vertical direction as well as the horizontal direction. The data capacity can be at a maximum of 7,250 numeric characters and 10,100 ASCII characters. HC2D barcodes use the Reed-Solomon [11] error correction, which can detect and correct multiple errors and HC2D barcodes have an option to compress data which allows a large amount of data to be stored [12]. HC2D barcodes can be read using a standard scanner and supporting software. The HC2D barcode has a greater capacity than other common 2D barcodes. Moreover, the shape of the HC2D barcode is suitable for use with paper documents or print media.

Table 1. The characteristics and properties of 2D barcodes.

	PDF417	Data Matrix	Maxi Code	QR Code	Aztec Code	HC2D barcode
						
Code type	Multi-low	Matrix	Matrix	Matrix	Matrix	Matrix
Capacity (Charac-	1,850	2,355	93	4,296	3,067	7,250

ters)						
Charac-teristic	High capacity	High capacity, small	High speed reader	High capaci-ty, small, high speed reader	High capacity	High capaci-ty, small,
Applica-tions	Office	Plant, medical industry	Industrial products import and export	All indus-tries	Aviation and transport industries	Paper-based Document

2.2 Cryptographic Hash Function

Cryptographic hash function is the hash function used for the purpose of safety information such as confirmation of identity to login (authentication) or to check the validity of the content, such as SHA-1 and MD5. Input data to the hash function can be varied in size and the hash function does not require any key. This result is called a hash value or a message digest with a fixed length and cannot be calculated back to the original message which is a one-way property. Hash function is often used for creating digital fingerprints which is used for checking whether or not the data has changed [13].

2.3 Digital Signature

Digital signature [14] is signature electronic that can be used to prove the identity of the sender or the signed document. It can verify the content of the message or data in document that it is an original and has not been altered or modified in transit. A digital signature can be done easily, but it cannot be mimicked, forged or modified by an unauthorized person because the digital signature uses asymmetric cryptography. This makes counterfeiting impossible and sender cannot deny responsibility (non-repudiation) of the information or document with the corresponding signature. The process of creating a digital signature is shown in Fig. 1.

The message is inputted to a mathematical process called a hash function to get a fixed-size data called message digest, because the original data is often very long which makes the signing process take longer. After that, the message digest is encrypted with private key of the sender. The signature can be used to authenticate the sender of the message since only the sender has knowledge of the private key. The encrypted message digest is called a digital signature. The digital signature is then sent to the recipient along with the original data.

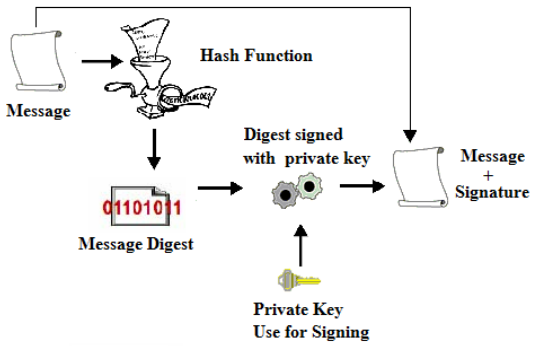

Fig. 1. The process of creating a digital signature.

In order to verify the digital signature, a message digest is derived through a hash function from the received data. The digital signature is decrypted with the sender's public key to obtain a message digest. Then, the two message digests are compared. If both values are identical, the data has not been modified and the signed message was sent from the owner of the public key. Hence, the sender cannot deny transmitting the message. However, if the values are different, it indicates that the received data has been modified during transit. The process of verifying a digital signature is illustrated in Fig. 2.

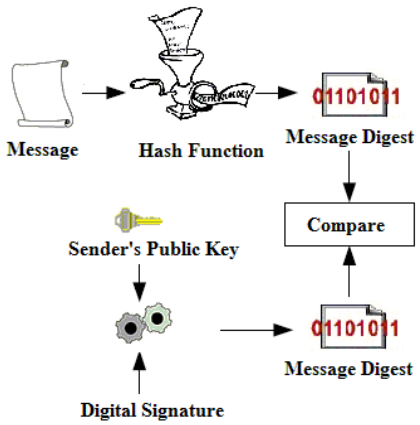

Fig. 2. The process of verifying a digital signature.

3 Design and Implementation

In this section, the design and implementation of an implementation of a paper based authentication using HC2D barcode and digital signature is presented. By using our

proposed method, the authentication of the paper-based document (plaintext) can be verified.

3.1 Sender Process

The sender prepares a message and starts the process of creating a digital signature. The message is passed through the hash function to obtain the corresponding message digest. The resulting value is then encrypted with the private key of the sender. The resulting value is a digital signature. Both original message and the digital signature are used in the process of creating HC2D barcode. The original message and HC2D barcode are then printed on the paper and the paper-based document can be sent to the recipient as shown in Fig. 3.

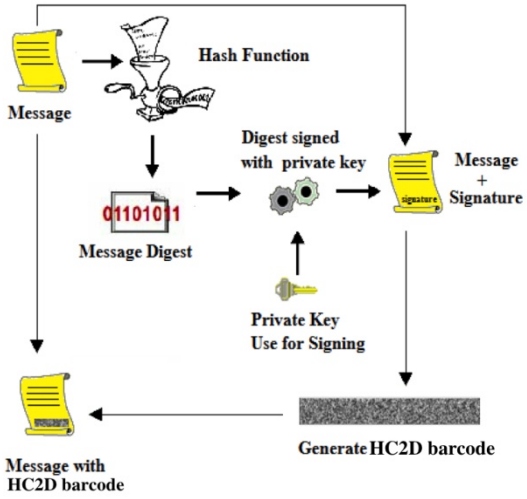

Fig. 3. The process of creating a paper-based authentication document using HC2D barcode and digital signature.

3.2 Receiver Process

When the recipient receives the document from the sender, the recipient can verify the authenticity of the document by the following process. The document is first scanned to obtain the image of the document. The verifying software reads the HC2D barcode and then obtains the data in the barcode using the Reed-Solomon error correcting code to detect and correct errors that may occur during shipping. The HC2D barcode may have been distorted or damaged. After successfully decoding using the Reed-Solomon error correcting code, the obtained data is decompressed (if data is compressed) to obtain the actual data which is a message from a sender and a digital signature. The digital signature part is decrypted with a public key. The message part is

inputted to the hash function to obtain the message digest. Both message digests are compared. If they are identical, the information in the barcode has not been altered.

The text on the document can be recognized using OCR function to obtain the original text of the document. The data is passed through the hash function to get message digest which is used to compare with the message digest obtained from the HC2D barcode. If both values are the same, the text on the document is accurate and has not been modified in transit. If they are different, it may be possible that the text on the document may have been modified during transit or may be possibly due to errors of the OCR. If this occurs, the recipient must visually compare the text on the document and the text in the HD2B barcode. The verifying software can overlay the documents or put them side by side and highlight the positions that are different. The verifying process is shown in Fig. 4.

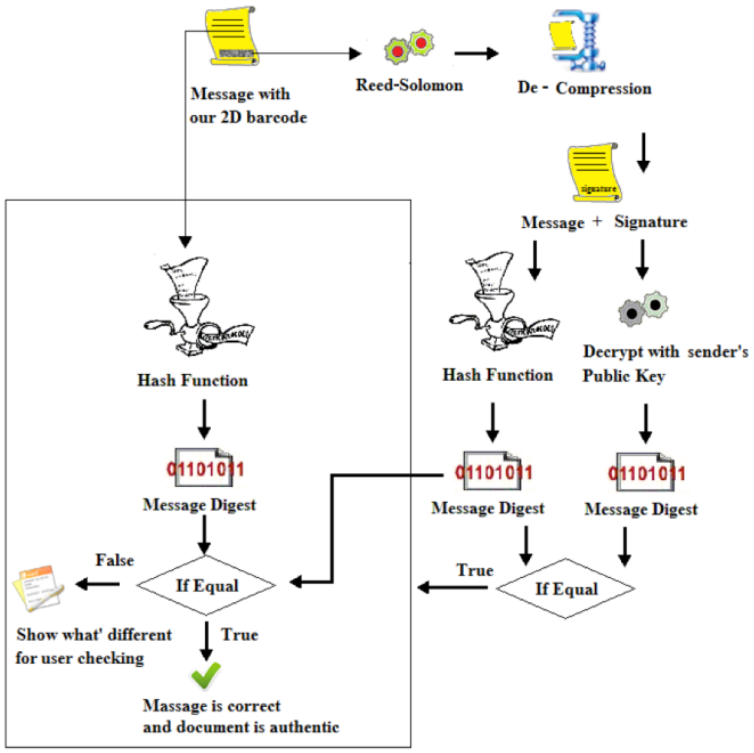

Fig. 4. The verifying process of the paper based authentication using HC2D barcode and digital signature.

4 Security Analysis

This research uses a digital signature technique to provide security of the data on the document. This is because the digital signature can be used to verify whether or not

the original content of the message or document has not changed or been modified in transit. The sender can efficiently create a digital signature. However, it is infeasible for an unauthorized person to modify the text or document and generate the digital signature as the sender. A digital signature is used for authentication because before the sender sends a message, the message digest of the message is encrypted with the sender's private key, which is only known by the sender, and only the sender's public key can be used to decrypt the digital signature. Successful digital signature verification implies that the message was actually sent by the sender and has not been modified in transit. As a result, the sender cannot deny responsibility for creating the message. This provides non-repudiation of the message since the sender has to encrypt the message digest with the corresponding private key. The capabilities of a digital signature, as mentioned above, would show that the digital signature also provides the integrity of the message; it ensures that message has not been modified in transit. If the message has been modified or changed during transit, the digital signature verification will fail. Using a standard algorithm and a proper key length, it is infeasible to create a fake digital signature of the message.

5 Experimental Results

To verify our design, we chose Java programming language (Java) for the development because it provides Java Cryptographic Architecture (JCA) which provides cryptographic functionality such as digital signature and digital certificate. The key tool is used for key storage, and this is in accordance with the certificate X.509. After the certificate is created, it can be exported and distributed. In a real life situation, a reputable Certificate Authority (CA) issues the digital certificate. For creating a digital signature of the message, we use SHA-256 [15] algorithm, which provides 256-bit output and RSA [16] algorithm which is used to sign and verify the digital signature.

Since official documents or common documents are often created with a word processor such as Microsoft Word, we chose Microsoft Word as input of the system. We also chose to use a two-dimensional bar code called HC2D barcode, which is designed for paper-based documents because its shape is appropriate for the attachment and print media. The HC2D barcode occupies less space than other 2D barcodes. Moreover, the HC2D barcode also provides data compression functionality which allows the barcode to store more data. The work is divided as the sender process and the recipient process. The process of the sender system is shown in Fig. 5.

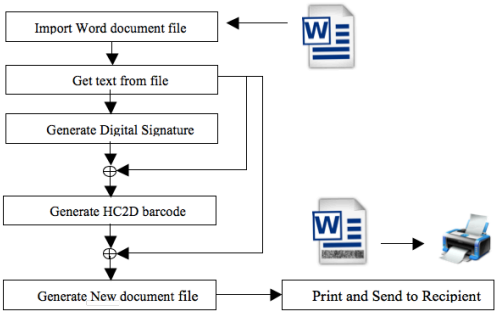

Fig. 5. The process of the sender system.

The process begins as the sender enters Microsoft Word file into the system. The software obtains the text from the document, and then the system will create a digital signature from text with sender's private key, generate a HC2D barcode containing the message and the digital signature, and finally attaches it to the message. A new document which consists of the original text and the HC2D barcode is generated and can be printed on paper. The process of the receiver system is shown in Fig. 6.

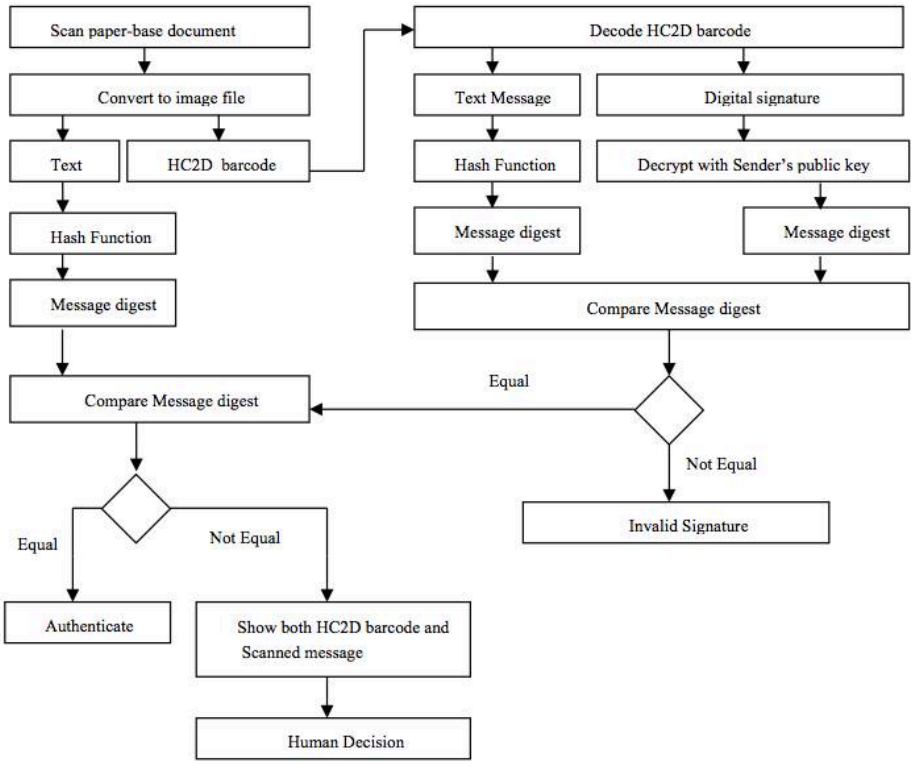

Fig. 6. The process of the receiver system.

When the recipient receives the document from the sender, the paper document must be scanned as an image. The image of the HC2D barcode is processed. The system will decode HC2D barcode to get the message and the digital signature. Then the digital signature which is read from HC2D barcode is decrypted with the sender's public key to obtain the message digest. The text message from HC2D barcode is passed through a hash function to obtain another message digest. Subsequently, both message digests are compared. If they are equal, the HC2D barcode contains the original message which was sent by the sender and has not been modified in transit. The printed text message on the paper is also read using OCR. The obtained text is hashed to obtain a message digest which is used to compare with the message digest from HC2D barcode. If both message digests are identical, the document is valid and has not been modified in transit. It also confirms that the document was actually sent by the sender who is the owner of the public key. On the other hand, if they do not match, it may be possible that the text on the document may have been modified during transit or may be possibly due to errors of the OCR. The system will display the differences between the two texts. This allows the user to visually verify them.

6 Conclusion

To determine the integrity of the data in the form of paper documents or published print media, a digital signature and a HC2D barcode can be used without relying on the database or file. The procedures and inspection processes can be performed automatically, if the OCR is accurate. Otherwise, a human is required to perform further verification. This research presents a process with semi-automatic in order to facilitate the review process. The verification starts with the automatic process. If the verification fails, software will show the difference between the data on printed documents and text from HC2D barcode for human inspection.

References

1. R.L. van Renesse, “Paper-based document security–A Review,” in European Conf. on Security and Detection, 1997
2. U. Garain and B. Halder, “On automatic authenticity verification of printed security documents,” 6th Indian Conf. on Comput. Vision, Graphics & Image Process., 2008, pp. 706-713.
3. J.Z. Gao, L. Prakash, R.Jagatesan, “Understanding 2D-BarCode Technology and Applications in M-Commerce – Design and Implementation of A 2D Barcode Processing Solution”, 31st Annual Intl . Computer Software and Applications Conference (COMPSAC 2007), Beijing, July 24-27, 2007.
4. M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code", International Proceedings of Computer Science and Infor-

mation Technology, ISSN 2010-460X, International Conference on Computer Engineering and Technology, pp. 94-98, vol. 40, 2012.
5. QR Code, http://www.denso-wave.com/qrcode/
6. Rong, C. et al.: Coding Principle and Implementation of Two-Dimensional PDF417 Bar code. In: 6th IEEE Conference on Industrial Electronics and Applications, pp. 466-468 (2011)
7. Ke, H., Zhang, G.: An Algorithm Correcting Flex Distortion of Aztec Code. In: 2nd IEEE International Conference on Information Management and Engineering, pp. 457-460 (2010)
8. Biao, L. (2007), A DataMatrix-based mutant code design and recognition method research. In: Proceedings of the 4th international conference on image and graphics, pp. 570-574, 2007
9. Data Matrix, http://en.wikipedia.org/wiki/Data_Matrix
10. P. Subpratatsavee and P. Kuacharoen, "An Implementation of a High Capacity 2D Barcode", Communications in Computer and Information Science, Springer, ISSN 1865-0929, 5th International Conference on Advances in Information Technology, pp. 159-169, vol. 344, 2012.
11. Mamidi, S. et al.: Instruction Set Extensions for Reed-Solomon Encoding and Decoding. In: 16th IEEE International Conference on Application-Specific Systems, Architecture Processors, pp. 364-369 (2005)
12. Islam, M.R., Ahsan Rajon, S.A.: An Enhanced for Lossless Compression of Short Text for Resource Constrained Devices. In: 14th International Conference on Computer and In-formation Technology, pp. 292-297 (2011)
13. M. Singh and D. Garg, “Choosing best hashing strategies and hash functions,” Int. Advance Computing Conf., 2009, pp. 50 – 55.
14. P. Kuacharoen, “Design and Analysis of Methods for Signing Electronic Documents Using Mobile Phones”, International Conference on Computer Applications and Network Security (ICCANS 2011), pp. 154-158, May 2011.
15. SHA-2, http://en.wikipedia.org/wiki/SHA-2
16. RSA Cryptography Standard, PKCS #1 v2.1, 2002.