International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 289-296
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

Trusted Document Signing based on use of biometric (Face) keys

Ahmed B. Elmadani
Department of Computer Science Faculty of Science Sebha University
Sebha Libya www.sebhau.edu.ly
elmadan@yahoo.com

ABSTRACT

An online secured document exchange, secured bank transactions, and other e-commerce requirements need to be protected in commercial environment as it becomes big,. Digital signature (DS) is the only means of achieving it. This paper introduces a prototype online-algorithm in signing and verifying a document digitally. Document's hash value is calculated, and protected using keys derived from face characteristics. This paper presents a method in signing document differ from traditional systems using passwords, smartcards or biometrics based on direct access. It utilizes a wirelessly accessed biometrics type to provide:

1. Un tampered biometrics in digital signatures.
2. Proof of a true identity.

It also investigates existing digital signature system that is based on smart card. The obtained results were translated in term of speed and security enhancement which is highly in demand of e-commerce society

Keywords

Digital Signature, Smart card, Hash, True identity and Biometric (face).

1. INTRODUCTION

A mathematical scheme for demonstrating the authenticity of a digital message or document is known as Digital Signature (DS) [1]. DS convince a recipient that a document was created by a known sender. DSs are commonly used for software distribution, financial transactions, and in other cases to avoid forgery and tampering [2]. Digitally signed messages may be anything that can be represented as a bit or a string, examples include electronic mail, contracts, or a message sent via some other cryptographic protocol [3]. Hash function is used in creating and verifying a DS. Hash function is an algorithm which creates a digital representation of document. Few hashing algorithms have been developed such Secure Hash Algorithm – 128 (SHA-1) and Message Digest Version 5 (MD5) to be used in e-commerce [4]. SHA-1 is a secured hash algorithm – 160. Produces 160-bit hash value. It is designed by NIST & NSA in 1993 revised 1995 as SHA – 160, US standard for use with digital signature algorithm (DSA) signature scheme. SHA-256, SHA-384, and SHA-512. Designed for compatibility with increased security provided by the advanced encryption standard (AES) cipher[3].

In traditional DS, normally a smart card is used to perform signatures because the used cryptographic keys are stored inside the card [6]. However most of the existing DS systems, provide signature without proofing true identity[5], because they stand on using keys that anyone can use[7]. Therefore, documents have to be signed in such a way that proofs the true identity to avoid many attacks reported in [8][11]. This can be done only by using user's personal characteristics such as fingerprint, Iris or face [7].

In automation security, faces are more secured than passwords, because of fine

differentiation between seemingly identical and won't be forgotten or stolen [9]. Faces are also more secured than fingerprint, because fingerprint can be spoof using jelly[10]. Face image as any digital image always needs to be enhanced, to come out with its features clearly. This is because of the low quality images captured using camera devices. An image once captured and resized, is filtered using one of the known filters methods such as Linear, Wiener, Median, or Gaussian [9]. The image using one or more filtering algorithm is filtered several times until it becomes clear. Then information can be constructed [12]. The constructed information are stored for future comparison use. Face structure is eyes, mouth, and there position, which are different from person to another. All related together forming a unique characteristic of face [9]. There are more factors that can be used, that might make recognition easy or difficult they are listed in the FERET dataset [15].

Several face recognition algorithms were introduced in recent years. One of them is to measure the resulted triangle between eyes and mouth, but this is trivial of change, so a measurement should be taken in age intervals [][16]. The first mention to eigenfaces in image processing, a technique that would become the dominant approach in following years, was made by L. Sirovich and M. Kirby in 1986, it is based on principal component analysis (PCA) [16]. It becomes a base of developing many new face algorithms such as the measurement of the importance of certain intuitive feature, geometric measures between eye distances, with length ratio [17].

This work considered as an improvement of the research done by Costas et al (2008), they perform face-based digital signature in retrieving video segments using pre-extracted face in detection and recognition[14]. They use signature in retrieving while in this work we use segments of document to retrieve their signatures for verification.

In our proposed DS system, we will introduce a system that uses keys derived from user's face that will help in assuring true identity, face factors mentioned in [15] are out of our concern. In our security analysis, we only consider secure signature-generation systems that use SMCs to protect DS from attacks mention in [8]. Then to improve the use of biometrics in order to proof true user identity as in [13], and DS protection. Meanwhile avoid using systems based on biometric which can be tampered such as fingerprint [14]. In the proposed system, we shall construct keys from face that is protected using a Ron's Code ver. 5 (RC5) a variable-key-size encryption algorithm. It is fast and suitable in protecting SMC keys [6]. Of course other solutions exist. However, they are out of the scope of this paper..

2. METHODOLOGY AND DISCUSSIONS

The following paragraphs will discuss proposed algorithm, experiment and obtained results.

2.1 PROPOSED ALGORITHM

Sequence of DS in the proposed system for any given document shown in Figure 1 are performed in five steps described as following:

- Enhancement, face image adjustment and filtering..
- Feature extraction, information extract and keys construction.
- Document signing, obtaining document fingerprint.

- Signatures protection, document and keys protection.
- Siging authenticity, signatures matching.

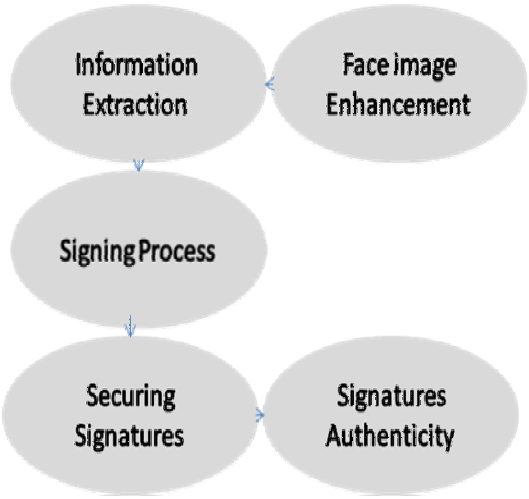

Figure 1. Sequence process in proposed system

2.2 FACE IMAGE ENHANCEMENT

At each sign-point, there is a fixed webcam that is used to capture face image.

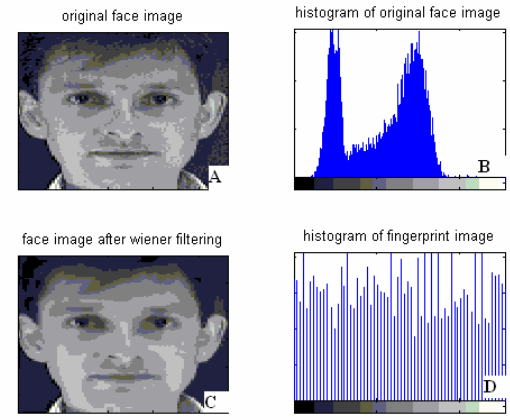

Figure 2. Face image enhancement, and noise remove using wiener filter

The selected area surrounds eyes, nose and mouth, within the dimension of 200x200 pixels. Figure 2 A shows an original image, while B presents the histogram of A, and it shows that information are not distributed, it has to be filtered. In C a face image is shown after removing noise by using fast Fourier transform (FFT) "wiener filter". It was used several times to come out with it features. The histogram of a well distributed information as a result filtering process was shown in D.

Face image is then cropped to dimension 150x150 pixels in an area reach of information. It contains eyes, nose, and mouth to use it for feature extraction as shown in Figure 3.

Figure 3. Selected face image area that is reach of information.

2.3 INFORMATION EXTRACTION

The cropped face image that prepared in paragraph 2.2 is used to extract features to calculate user key **(** key_s as sender's key and key_r receiver's key**).** User key are calculated using an equation (1).

$$key_s = \sum_{i=j=0}^{n,m} x_1(i,j)$$
$$key_r = \sum_{i=j=0}^{n,m} x_2(i,j) \quad (1)$$

Where x_1 and x_2 are sender's, receiver's cropped face image 160x160 pixels and $i = 0...n, j = 0..m$.

Obtained users keys are unique as results of applying the equation (1). Table 1 shows obtained users keys, it is insure that users can be distinguish from each other.

As a requirement of signing process, user requires another key (key_{sr}), it is constructed after selecting a target user as a receiver of a document.

Table 1. Users keys

User No.	User key (key_s or key_r)
6	581497
7	533018
8	668856
9	627684
18	632414

The key is constructed by combining the two keys (key_s and key_r) using equation no. (2). The constructed key (key_{sr}) is used in encryption process.

$$key_{sr} = key_s i, key_r j$$
$$where \; i = 1 \; n, \; j = n+1 \; n+m \qquad (2)$$

The constructed key_{sr} is used in both sides for encryption or/decryption and to protect an outgoing document in sender's side or incoming document in receiver's side. A third column in Table 2 shows results of applying equation (2) to construct a key (key_{sr}) that is used in an encryption process.

Table 2. Constructed key key_{sr} between sender and receiver

Sender's key (key_s)	Receiver's key (key_r)	Combined key's (key_{sr})
581497	7533018	5814977533018
7533018	581497	7533018581497
668856	668856	668856668856
627684	632414	627684632414
632414	627684	632414627684

2.4 SIGNING PROCESS

A user who intends to sign a document (**Doc**) has to first select or prepare a document, then a process using equation no. (3) to calculate a fingerprint of the document. SHA-1 as stable hash algorithm was chosen to calculate document's fingerprint. Then a sender invokes RC5 algorithm with a constructed key (key_{sr}) to encrypt the calculated fingerprint as shown in equation (4).

$$\text{Fingerprint} = \text{SHA-1}(\textbf{Doc}) \qquad (3)$$
$$\text{Encrypted-fingerprint} = \text{RC5}^{key_{sr}}(\text{fingerprint}) \qquad (4)$$

Sender prepares a message that contains document, its fingerprint and sender's key and sent them to the receiver according to the equation no. (5) and as shown in Figure 4.

$$\text{Message} = (\text{Encrypted-fingerprint, Doc, } key_s) \qquad (5)$$

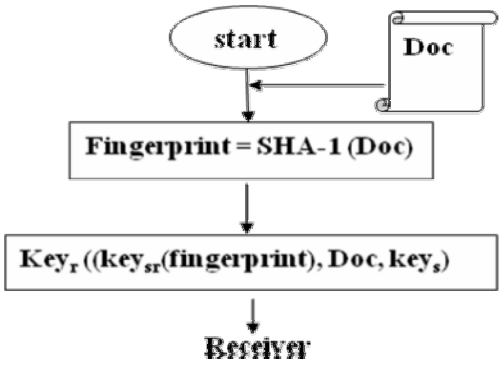

Figure 4. Sequence process of a document signing and message encryption

2.5 SECURE SIGNATURES

To avoid un authorized use of document and used keys in signatures, a RC5 cryptographic algorithm is used to protected them. Message contains document (Doc), fingerprint and keys are prepared by sender and protected using a formed key (key_{sr}) that only target

receiver can decrypt according to the equation (6).

$$\text{Encrypted-Mseg} = \text{RC5}^{key_{sr}}(\text{Message}) \quad (6)$$

2.6 AUTHENTICITY of SIGNATURES

Verification process is performed in the receiver's side, receiver once he received an encrypted message, he decrypts it using his key (key_r) to obtain original document, sender's key (key_s), and encrypted fingerprint. Two processes are used one to calculate new fingerprint and second to construct combined key (key_{sr}) as discussed in **2.3**. The key is used to decrypt the received encrypted fingerprint. Signature is authenticated by comparing the two obtained fingerprints. A document is said authenticated and sent by trusted person if fingerprint are equals. In Figure 5

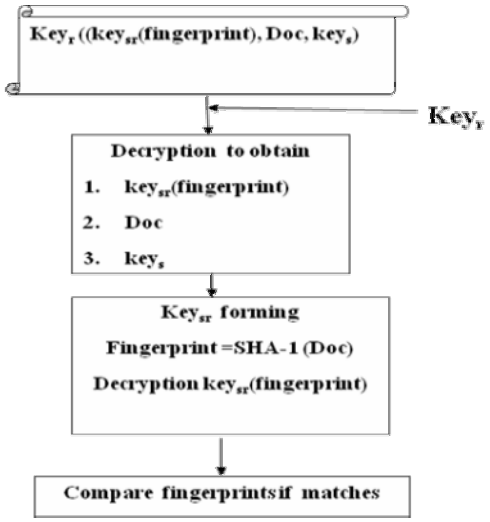

Figure 5 Received message decryption and signing authentication process.

illustration of verification process starts by the decrypting of the received message with receiver's key to obtain the sender's key (key_s). The key_s will be used to construct a combination key (key_{sr}) that needed to decrypt received fingerprint. Receiver calculates fingerprint of received document using SHA-1 algorithm and compare the two fingerprints to see if they match.

2.7 TESTING THE ALGORITHM

Two signature points are configured using two connected computers where each was equipped with webcam. They are used to test the proposed algorithm. One is for document signing, where the second is for signature verification. The system was tested for acceptance and rejection in term of signature-verification running process. This test is used to discover the system's incorrect decision. Use was made of 1030 matching trails (MT) and three security levels. Table 3 shows used intensity level for each of the three levels security. Group (1) uses 30 low intensity face images, group (2) uses 400 medium intensity face images, where group (3) uses 600 high intensity face images.

Table 3 Number of Recognized-Rejected users by the proposed system

Group / Description	Group (1) Low	Group (2) medium	Group (3) High	Total
Number of Users	30	400	600	1030
Recognized	28	393	592	1013
Rejected	2	7	8	17
Recognized Rate	93.33	98.25	98.67	98.35
Error Rate	6.67	1.75	1.33	1.65

The results of testing for the system to the MT, for group 1 a 28 out of 30 low intensity images were recognized, that is 93.33%. Meanwhile, 2 images were rejected with 6.67% as demonstrated in Figure 6.

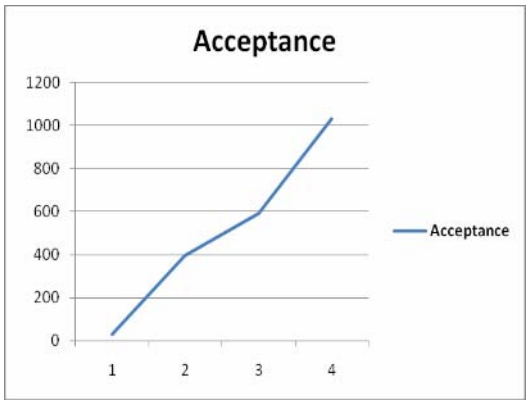

Figure 6 Accepted users by the proposed system

In group 2 which presents medium intensity face images as shown in Figure 7, 393 out of 400 face images, were recognized with percentage of 98.25% and only 7 images were rejected with percentage of 1.75%.

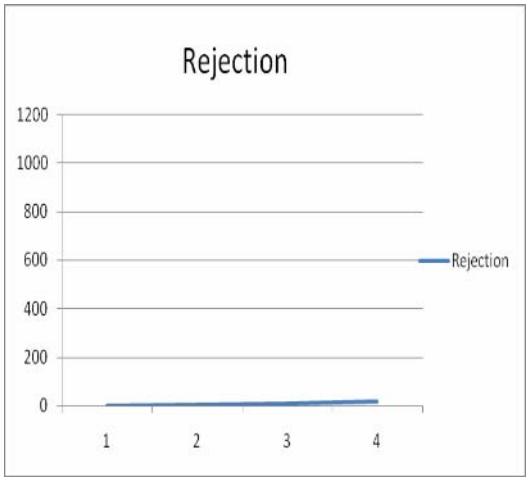

Figure 7 Rejected users by proposed system

In group 3, 600 high intensity face images were used as shown in Figure 8, 592 were recognized registering a 98.67% and 8 rejection, that is 1.33%.

In summary 1030 face images were used, images got different intensity. 1013 of them were recognized with percentage of 98.35%, and only 17 of them were rejected, that is 1.65% and this demonstrates the success of the proposed system.

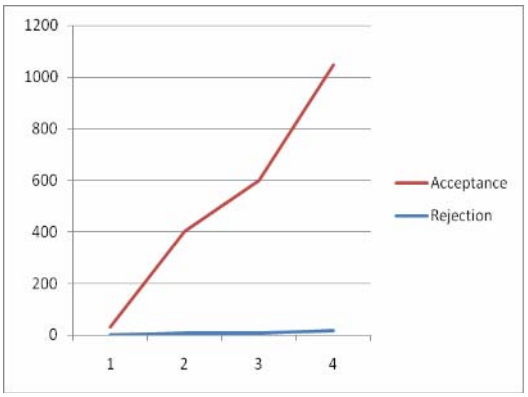

Figure 8 Accepted and rejected users by the proposed system

In Table 4 tests of the proposed system done only for known users, the false acceptance rate (FAR) registered value equals to zero in all groups. The false rejection rate (FRR) goes in descending order which means configuring the system with big number of users will translate in getting less rejection as results show for low and all intensity.

Table 4 FAR and FRR Ranges

No.	Description	FAR	FRR
1.	Low intensity	0	6.67
2.	Medium intensity	0	1.75
3.	High intensity	0	1.33
4.	For all intensity	0	1.65

2.8 THIS ALGORITHM AGAINST EXISTING ALGORITHMS

In recent years few algorithms are developed to solve document signing digitally, but they fail in covering a lot of issues. The proposed algorithm solves them as will be described below.

Most of DS systems as in Sufreenmohd at el (2002) or in Elmadani at el (2005) are using smart card to store keys and they suffer from forgery or tampering, were the proposed algorithm solve this problem by authenticating user with their faces, that were stolen, forgotten, tampered and user has nothing to carry with a hand. The existing DS algorithms as in Sirovich and

Kirby (1987) are based on temple selection in extracting features, Givens at el (2003) and Yang (2010) algorithms are based on calculating values from image to compare them later with storing ones, such processes are time consuming, were in the proposed system features are based on forming keys which are numbers, directly processed no need to store them, which means protection from any attack mentioned by Langweg (2006). The proposed algorithm uses simple mathematic functions in key calculation different than algorithms used by Costas at el (2008) or used by Kirby and Sirovich (1990), our system is fast because it is based calculating numbers, it requires minor process, less memory space compared to them.

3. COCLUSION

A model of signing – verifying document signature and protecting it was presented. Meanwhile, an investigation and drawback of existing digital signatures were shown. The proposed algorithm uses person characteristics biometrics (face) which is not possibly stolen or forge or tampered. It provides an easy method in use, that requires nothing to carry with. Our results shows that with no doubt, face is strongly recommended for online document signing.

4. REFERENCES

1. Nentwich F, Kirda E and Kruegel C. Practical Security Aspects of Digital Signature Systems. Technical University Vienna. Technical. 2006.
2. Introduction to digital signature. www.e-signature.gov.eg/ ElectronicSignature_Mechanizm_Arabic. 2010.
3. Robshow M. MD2, MD5, SHA and other Hash Functions. RSA Laboratories Technical Report TR-101.1995.
4. Wang X, Feng D, Lai X and Yu. Collision for Hash Functions MD4, MD5, HAVAL-128, and RIPEDMD. Proceedings of the 2th Annual International Cryptology Conference (Crypto ’04), Santa Barbara CA. 2004.
5. Elmadani. A. B. Digital Signature forming and keys protection based on person’s Characteristics. Proceedings of the IEEE International Conference on Information Technology and e-services (ICITeS’2012). Souse, Tunisia. 2012.
6. Elmadani A. B, Prakash V and Ramli A. R. Application of Smartcard & Secure Coprocessor, BICET conference. Brunei.2001.
7. Elmadani A. B. Human Authentication using FingerIris algorithm based on statistical approach the 2nd International in network digital conference (NDT '10), Prague Czech Republic. pp (288-296). 2010.
8. Spalka A. Cremers A and Langweg H. Protecting the Creation of Digital Signature with Trusted Computing Platform Technology Against Attacks by Trojan Horse. In IFIP Security Conference. 2001.
9. Fang, Y. Wang Y and Tan T. Combining Color, Contour and Region for Face Detection. ACCV2002: The 5th Asian Conference on Computer Vision, Melbourne, Australia. 2002.
10. Elmadani A. B, Prakash V, Ali, B. M, Ramli A. R and Jumari K. Fingerprint Access Control with Anti-spoofing Protection, Brunei Darussalam Journal of Technology and Commerce. Brunei. 2005.
11. Langweg H. Malware Attacks on Electronic Signatures Revisited. In Sicherheit 3rd Jahrestagug Fachbereich Sicherheit der Gesellschaft fuer Informatik. 2006.
12. Zhao W, Chellappa R, Phillips P. J and Rosenfeld A. Face Recognition: A Literature Survey. ACM Computing Survey. Vol. 35, no. 4. PP. 399–458. 2003.
13. Yang J. Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System. Proceedings of Fourth International Conference on Management of e-Commerce and e-Government (ICMeCG), pp. 405-420. China.2010.
14. Costas C, Nikolaidis N and Ioannis P. Face-based Digital Signatures for Video Retrieval. IEEE Transactions on Circuits and Video Technology, Vol. 18. No. 4. Pp. 549-553. 2008.
15. Givens G, Beveridge J, Bruce A, Draper B and Bolme D. A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces. Proceedings of Computer Vision and Pattern Recognition Workshop (CVPRW’03). Wisconsin USA. 2003.

16. Sirovich Land Kirby M. Low-dimensional procedure for the characterization of human faces. Journal of the Optical Society of America A - Optics, Image Science and Vision, Vol 4. No 3. pp 519–524. 1987.
17. Kirby M and Sirovich L. Application of the karhunen-loeve procedure for the characterization of human faces. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 12. No. 1. Pp 103–108. 1990.

Ahmed B. Elmadani was born in Libya 1956. He received Ph.D. degree at UPM University Malysia in 2003. He worked in computer science department Faculty of Science Sebha University (Libya), from 1997 to 1999 as Assistant lectuerar and head department of computer Science, from 2003 – 2008 as lectuerar at the same department, from 2009- till now as asistant prof. and Vice Dean at the same Faculty. His main research interests include cryptography, information security, imaging, digital signature and biometrics fingerprint.