

SYSTEM AND METHOD FOR SIGNING A COMPUTER DOCUMENT

FIELD OF THE INVENTION

The field of the invention relates to signing of documents readable in a computing device, as well as the authentication of such signatures.

BACKGROUND OF THE INVENTION

In today's global society connected by the Internet and the increasing use of mobile communication devices, such as smartphones and tablets, the exchange of documents within the online domain becomes more frequent and common. These documents can be in any electronic format, such as Microsoft Word or Portable Document Format (PDF). These documents may require application of signatures thereto before being sent out so that the recipients of such documents can verify their authenticity. Such signatures may be in the form of the usual handwritten signatures, or in the more traditional form of biometric signatures like fingerprints and/or thumbprints. Signatures may also comprise both a handwritten signature and a biometric signature. Handwritten signatures alone are inconsistent, while true biometric signatures like fingerprints may be more consistent. The problem with handwritten signatures is that they can be highly unreliable and inconsistent, especially if the person signing is having a bad day or is under pressure. It may also be difficult to accurately ascertain the accuracy and authenticity of such signatures. It is increasingly common today that signed documents are sent online instead of by the traditional snail mail or courier, and unless the original copies are absolutely required, soft copies of the documents are transmitted electronically. The documents can comprise anything ranging from simple acknowledgement letters to sensitive personal or corporate information.

A common method of signing a document and sending it electronically is to print out the document, verify its contents, and then signing on the document. The original signed document is often kept in a safe place. If the document contains more than one page, the signature can be on one page (typically the final page), all of the pages, or any number of pages in between. Subsequent to being signed, the document is scanned into the computer and

then sent out by email. However, during the scanning of the signed document, the document is likely to be prone to tampering. This is especially so if the document contains more than one page. One example of tampering is the insertion of additional pages which the signing party (signatory) is not aware of, or the omission of some pages during scanning. Another example would be that a person skilled in the art can extract the signature from the document and embed it into another document, thereby imposing as the signatory.

Another common method is to graphically embed a signature directly onto a document electronically before sending it out. This solves the problems of insertion and deletion of pages and but it may also be vulnerable to extraction of the signature. In addition, the signatory can verify the contents of the document before placing a signature on it. However, the problem of extracting the signature and embedding it in another document still applies here. Another disadvantage is that there will not be an original copy signed by pen, i.e. wet signature; it will be difficult to verify the authenticity of the signature when it comes to contention, especially in cases involving important legal documents.

To overcome these problems, the graphically signed document can be encrypted with a digital signature. The first step in digitally signing a document involves hashing the document to generate a hash or digest of the document. This hash or digest is a shortened version of the document so that it can be encrypted faster. Although is it not technically required to perform the hashing function, the process of encrypting the entire document is often too slow to be feasible. The second step involves encrypting the hash or digest with a private key that belongs to the sender. In order to decrypt the hash or digest, the recipient needs to use a public key that is made available to him or her. Each private key for encryption has a corresponding public key for decryption. In other words, the sender must first provide to the recipient the public key necessary to decrypt the encrypted electronic document. If the public key does not match the private key, there will not be any authentication between them and the document cannot be decrypted. This method of encryption is commonly known as digital signing.

The advantage digital signing offers over traditional signing by pen is that digital signatures can only be created by the intended signatory, assuming his or her private key is kept secret.

If access to the private key is made available to parties other than the signatory, the said parties can impose as the signatory and digitally sign documents, akin to the way traditional signatures are often forged by experts. However, one major issue of digital signatures is that the corresponding public key must be used before the document can be opened and read.

- 5 Therefore, there has to be a pre-existing relationship or exchange of keys between the sender and the recipient prior to the digital signing and encryption and decryption of documents that are encrypted with a digital signature.

10 The Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (ESIGN) specify what constitutes a valid and legally binding electronic signature. Specifically, an electronic signature is a sound, symbol, or process associated with a computer document, such that it is unique to the signatory, under the sole control of the signatory, linked to the document in such a way as to prevent tampering, and capable of being authenticated.

15

Without the implementation of separate infrastructure software, the signed document may fall short of the third requirement “linked to the document in such a way as to prevent tampering”. With respect to digital signatures, the signed document may fall short of the second requirement “under the sole control of the signatory” if the private key is unintentionally disclosed, and this in turn leads to issues with the fourth requirement “capable of being authenticated”.

25 In view of the above-mentioned problems and the legal aspect, there exists a need to combine the advantages of traditional signatures and digital signatures in a single signing mechanism for computer documents in order to meet the legal requirements. Accordingly, it would be desirable for a signatory to intentionally and manually perform the signing on a computer document with a handwritten and/or biometric signature, and encrypting the computer document with a digital signature.

30

SUMMARY OF THE INVENTION

The invention solves one or more of the above-mentioned problems. The invention provides a system and method for digital signing of computer documents which uses a two-factor signing sequence to combine the advantages of handwritten and/or biometric signatures, and digital signatures, together in a single signing mechanism. Advantageously, the invention allows for the signature to be unique to the signatory and under the sole control of the signatory (in the handwritten/biometric signature), and as such ensures that there can be no substitute of the signatory by a proxy. The invention further allows for the signature to be linked to the computer document such that the document cannot be tampered and for the signature to be authenticated in two factors (handwritten/biometric signature and digital signature). As such, the invention provides for compliance with the conditions of making a signed computer document valid and legal binding.

According to a first aspect of the invention, there is provided a method for digitally signing an unsigned document in a computing device communicable with a human interface device, wherein the unsigned document is readable by the computer device. The method comprises the steps of: receiving a first signature information generated from a first signature provided by a user to the human interface device during interaction therewith, the first signature information being descriptive of and characterizing the first signature provided by the user; generating a graphical rendition of the first signature from the first signature information.

The method further comprises either

- (i) hashing the unsigned document to generate a first hash; encrypting the first hash with a private key; and combining the unsigned document, the first signature information, and the encrypted first hash into a signed document, or
- (ii) combining the unsigned document and the first signature information into a marked document; hashing the unsigned document to generate a first hash; encrypting the first hash with a private key; and combining the marked document and the encrypted first hash into a signed document.

The resultant signed document displays the graphical rendition of the first signature when viewed with the computing device.

According to a second aspect of the invention, there is provided a system for digitally signing an unsigned document. The system comprises a human interface device communicable with a computer device, wherein the unsigned document is readable by the computer device. The system further includes means for receiving a first signature information generated from a first signature provided by a user to the human interface device during interaction therewith, the first signature information being descriptive of and characterizing the first signature provided by the user; means for generating a graphical rendition of the first signature from the first signature information.

10 The system further comprises either

(i) means for hashing the unsigned document to generate a first hash; means for encrypting the first hash with a private key; and means for combining the unsigned document, the first signature information, and the encrypted first hash into a signed document, or

15 (ii) means for combining the unsigned document and the first signature information into a marked document; means for hashing the unsigned document to generate a first hash; means for encrypting the first hash with a private key; and means for combining the marked document and the encrypted first hash into a signed document.

The resultant signed document displays the graphical rendition of the first signature when viewed with the computing device.

20

The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features will become apparent by reference to the following detailed description.

25

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the invention will now be described by reference to the accompanying drawings. The illustrative embodiments described in the detailed description, claims, and drawings are not meant to be limiting. Other embodiments may be utilized, and other changes
5 may be made, without departing from the spirit or scope of the subject matter presented herein.

FIG. 1 shows a schematic of the human interface device being in communication with the computing device.

FIG. 2 shows a flowchart of the method of digitally signing an unsigned document.

10 FIG. 3 shows one of the steps in the method of digitally signing an unsigned document.

FIG. 4 shows another of the steps in the method of digitally signing an unsigned document.

FIG. 5 shows one of the steps in the authenticating a signed document.

FIG. 6 shows another of the steps in the authenticating a signed document.

FIG. 7 shows a system implementing the method of digitally signing an unsigned document.

15 In the drawings, like parts are denoted by like numerals.

A preferred embodiment of the invention provides a method 100 for digitally signing an unsigned document. The method 100 occurs in a computing device 20 or computer that is communicable with a human interface device 22. The human interface device 22 can be a
20 tablet device comprising a touch-sensitive portion 24, such as a Topaz tablet, or a similar electronic device that comprises a similar touch-sensitive portion 24. The touch-sensitive portion 24 is capable of accepting actions performed on it by a person (alternatively known as user or signatory), such actions including but not limited to, making a handwritten signature and a biometric fingerprint. The tablet device may further comprise a stylus for ease of
25 writing or making the signature. The human interface device 22 can be connected to the computing device 20 via a computer interface connector 26 such as a USB connector for communicating with the computing device 20. The computing device 20 is capable of reading, viewing and displaying, among other things, the unsigned document.

In the embodiment, the method 100 comprises the step 102 of receiving a first signature information generated from a first signature provided by a user to the human interface device during interaction by the user with the human interface device. The first signature information is descriptive of the first signature provided by the user and is capable of characterizing the first signature. The first signature can be a normal handwritten signature or a biometric fingerprint or both. The method comprises the step 104 of generating a graphical rendition of the first signature from the first signature information. The graphical rendition of the first signature is a digitalized form of the first signature such that it can be received and read by the computing device. The method further comprises the step of either (i) 106 or (ii) 108 as described in the following.

(i) The step 106 comprises the sub-step 110 of hashing the unsigned document to generate a first hash. The first hash is essentially a shortened digest of the unsigned document which is unique enough such that it is almost impossible for two different documents to yield the same hash. The hash lessens the computational load in encrypting the document and expedites the process. The step 106 further comprises a sub-step 112 of encrypting the first hash with a private key. The private key is used in Public-Key Infrastructure (PKI) which is a well-known cryptography application with digital signatures. There is a public key corresponding to the private key, and both keys are related by a one-directional mathematical function, such that one key is unique to the other. The private key is normally kept secure by the signatory and only used when necessary to encrypt a document with a digital signature. The step 106 further comprises the sub-step 114 of combining the unsigned document, the first signature information, and the encrypted first hash into a signed document. Essentially, the signed document now comprises the original unsigned document and the first hash that has been encrypted with the private key, as well as the first signature information. The first signature information and the first hash provide the information necessary to verify the first signature in subsequent authentication processes.

(ii) The step 108 comprises the sub-step 120 of combining the unsigned document and the first signature information into a marked document. The step 108 further comprises the sub-step 122 of hashing the marked document to generate a first hash. The first hash is essentially a shortened digest of the marked document which is unique enough such that it is almost impossible for two different documents to yield the same hash. The hash lessens the computational load in encrypting the document and expedites the process. The step 108 further comprises a sub-step 124 of encrypting the first hash with a private key. The private key is used in Public-Key Infrastructure (PKI) which is a well-known cryptography application with digital signatures. There is a public key corresponding to the private key, and both keys are related by a one-directional mathematical function, such that one key is unique to the other. The private key is normally kept secure by the signatory and only used when necessary to encrypt a document with a digital signature. The step 108 further comprises the sub-step 126 of combining the marked document and the encrypted first hash into a signed document. Essentially, the signed document now comprises the marked document and the first hash that has been encrypted with the private key, as well as the first signature information which was previously combined with the unsigned document to generate the marked document. The first signature information and the first hash provide the information necessary to verify the first signature in subsequent authentication processes.

Consequent to either of the aforementioned two steps 106 and 108, the signed document displays the graphical rendition of the first signature when viewed with the computing device. With the digitalized form of the first signature obtained from the human interface device, the graphical rendition of the first signature is graphically embedded on the signed document such that when viewed with the computing device, the computing device displays the document with the graphical rendition of the first signature. This advantageously allows a person to visually see that the document has indeed been signed by a signatory with a handwritten and/or biometric signature.

Preferably in the embodiment, the first signature information comprises a first plurality of characteristics, and the plurality of characteristics comprises at least one of speed, direction, and fidelity of the first signature. The speed relates to the duration of time taken by the user in making a handwritten signature. The direction relates to the different strokes used by the user in making a handwritten signature. The fidelity relates to the visual details of the handwritten signature, or in the case of a biometric fingerprint, the line and shape characteristics of the biometric fingerprint.

Preferably, the embodiment comprises a method of transmitting the signed document to a recipient. Once a user or signatory has signed a computer document, the document can be sent or transmitted to another person, i.e. the recipient. The transmission can be, but not limited to, by email or internet file transfer.

Preferably in the embodiment, the signed document is capable of being authenticated by the recipient using, either step (i) 130 or step (ii) 132, or both steps 130 and 132 in any sequence. The steps are described in the following.

(i) The step 130 comprises the sub-step 140 of generating a second hash of the signed document. In a similar hashing function as generating the first hash described above, the recipient generates a second hash of the signed document locally in the recipient's computer. The second hash is independent of the first hash. The step 130 further comprises the sub-step 142 of decrypting the encrypted first hash with a public key, wherein the public key is corresponding to the private key as described above. The public key is made available to the recipient by the signatory and/or made available for retrieval by the public. The step 130 further comprises the sub-step 144 of comparing the second hash with the decrypted first hash. If both hashes match, then the digital signature in the signed document is authentic.

(ii) The step 132 comprises the sub-step 150 of comparing the first signature information in the signed document with a database. The database stores a plurality of second

signature information. The second signature information describes and characterizes a second signature. As every second signature information in the plurality of second signature information is different from one another, each second signature information describes and characterizes a different second signature. In order to describe and characterize a second signature, each second signature information comprises a second plurality of characteristics, wherein the second plurality of characteristics comprises at least one of speed, direction, and fidelity of the second signature. Each parameter in the second plurality of characteristics is described as per the parameters in the first plurality of characteristics described above. At least one of the abovementioned parameters is compared between the first signature information and the second signature information. The step may further provide for informational alerting to indicate whether the comparison results in a positive match or a negative match.

15 The authentication can also be performed by a third party who is neither the signatory nor the recipient of the signed document in question. Especially in events of contention wherein the veracity and authenticity of the signature is in dispute, or in litigation matters, the need for an authoritative verification of the signature arises. In most cases involving paper documents with handwritten signatures, the comparison is often done by visual sighting which can be

20 somewhat inaccurate, and even more so if there is intended forgery and the forger is an expert in this field. Moreover, in today's world, computer documents are being exchanged frequently and any intended forger can hide behind the computer and impose as the intended signatory. Therefore, it is necessary for signed computer documents to be capable of being authenticated.

25 Preferably, the embodiment also provides a method for edit-protecting the signed document in response to combining the unsigned document and the encrypted first hash into the signed document. Once the document is edit-protected, modifications of the edit-protected document cannot be performed without any advanced computing techniques. By edit-protecting the signed document, the recipient can be certain that the signed document received indeed

30 originated from the signatory and there has not been any alteration or tampering of the document during transmission. If there has been any alteration or tampering, or any transmission error, the content of the signed document would be changed and the second hash

generated from the signed document by the recipient would not match with the first hash, thereby not authenticating the signed document. To remove the edit-protection in the document, the method may further comprise the step of removal by using the same signature to be made by the same signatory.

5

Preferably in the embodiment, each of the first signature and the second signature comprises a handwritten signature, a biometric signature, or both. A handwritten signature is described as a signature made by a signatory's hand, i.e. a wet signature on paper. A biometric signature can be, but not limited to, fingerprints and/or thumbprints belonging to the signatory.

10

Preferably in the embodiment, the unsigned document, the marked document, the signed document, and any other variants of documents are in PDF.

15

The method 100 in the above embodiment may be implemented in a system 200. The system provides the means for performing each method and/or step and/or sub-step as described in the above embodiment.

20

While various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, within the scope and spirit of the disclosure being indicated by the following claims.

CLAIMS

1. In a computing device communicable with a human interface device, a method for digitally signing an unsigned document readable by the computing device, the method comprising:
 - receiving a first signature information generated from a first signature provided by a user to the human interface device during interaction therewith, the first signature information being descriptive of and characterizing the first signature provided by the user;
 - generating a graphical rendition of the first signature from the first signature information; and
 - one of:
 - hashing the unsigned document to generate a first hash; encrypting the first hash with a private key; and combining the unsigned document, the first signature information, and the encrypted first hash into a signed document, and
 - combining the unsigned document and the first signature information into a marked document; hashing the marked document to generate a first hash; encrypting the first hash with a private key; and combining the marked document and the encrypted first hash into a signed document,wherein the signed document displays the graphical rendition of the first signature when viewed with the computing device.
2. The method according to Claim 1, the first signature information comprising a first plurality of characteristics, the plurality of characteristics comprising at least one of speed, direction, and fidelity of the first signature.
3. The method according to Claim 1 or 2, further comprising transmitting the signed document to a recipient.
4. The method according to Claim 3, wherein the signed document is authenticated by the recipient with at least one of:
 - generating a second hash of the signed document; decrypting the encrypted first hash with a public key, the public key corresponding with the private key; and comparing the second hash with the decrypted first hash, and

- 5 ii. comparing the first signature information in the signed document with a database, the database comprising a plurality of second signature information, each in the plurality of second signature information being descriptive of and characterizing a second signature and comprising a second plurality of characteristics, and the second plurality of characteristics comprising at least one of speed, direction, and fidelity of the second signature.
- 10 5. The method according to any preceding claim, each of the first signature and the second signature comprising at least one of a handwritten signature and a biometric signature.
6. The method according to Claim 5, wherein the biometric signature is a fingerprint of the user.
- 15 7. The method according to any preceding claim, the method further comprising edit-protecting the signed document.
8. The method according to any preceding claim, wherein each of the unsigned document, the marked document, and the signed document is in Portable Document Format (PDF).
- 20 9. A system for digitally signing an unsigned document, the system comprising:
 a computing device and a human interface device, wherein the computing device is communicable with the human interface device and the unsigned document is readable by the computing device;
- 25 means for receiving a first signature information generated from a first signature provided by a user to the human interface device during interaction therewith, the first signature information being descriptive of and characterizing the first signature provided by the user;
- 30 means for generating a graphical rendition of the first signature from the first signature information; and
 one of:
 i. means for hashing the unsigned document to generate a first hash;
 means for encrypting the first hash with a private key; and means for combining the

unsigned document, the first signature information, and the encrypted first hash into a signed document, and

ii. means for combining the unsigned document and the first signature information into a marked document; means for hashing the marked document to generate a first hash; means for encrypting the first hash with a private key; and means for combining the marked document and the encrypted first hash into a signed document,

wherein the signed document displays the graphical rendition of the first signature when viewed with the computing device.

10. The system according to Claim 9, the first signature information comprising a first plurality of characteristics, the plurality of characteristics comprising at least one of speed, direction, and fidelity of the first signature.

11. The system according to Claim 9 or 10, further comprising means for transmitting the signed document to a recipient.

12. The system according to Claim 11, wherein the signed document is authenticated by the recipient, the authentication comprising at least one of:

i. means for generating a second hash of the signed document; means for decrypting the encrypted first hash with a public key, the public key corresponding with the private key; and means for comparing the second hash with the decrypted first hash, and

ii. means for comparing the first signature information in the signed document with a database, the database comprising a plurality of second signature information, each in the plurality of second signature information being descriptive of and characterizing a second signature and comprising a second plurality of characteristics, and the second plurality of characteristics comprising at least one of speed, direction, and fidelity of the second signature.

13. The system according to any one of Claims 9 to 12, each of the first signature and the second signature comprising at least one of a handwritten signature and a biometric signature.

14. The system according to Claim 13, wherein the biometric signature is a fingerprint of the user.

5 15. The system according to any one of Claims 9 to 14, the system further comprising means for edit-protecting the signed document.

16. The system according to any one of Claims 9 to 15, wherein each of the unsigned document, the marked document, and the signed document is in Portable Document Format (PDF).

10