

DIGITAL FILE ANTI-FORGERY PROTECTION**TECHNICAL FIELD**

5 The present invention relates to the technical field of protection of digital data against forgery or tampering, and traceability of digital files.

BACKGROUND ART

10 The patent application EP 3 031 169 A1 discloses at least one node in a distributed hash tree document verification infrastructure which is augmented with an identifier of an entity in a registration path. A data signature, which includes parameters for recomputation of a
15 verifying value, and which is associated with a digital input record, will therefore also include data that identifies at least one entity in the hash tree path used for its initial registration in the infrastructure.

20 The patent application EP 3 820 712 A1 discloses a solution for securing an article against forgery and falsifying of its associated data, and particularly of data relating to its belonging to a specific batch of articles, while allowing offline or online checking of the authenticity
25 of a secured article and conformity of its associated data with respect to that of a genuine article.

 The patent application WO 2010/0112101 A1 discloses a digital document which is protected through:
30 receiving the digital document; receiving associated data

comprising at least partially data from the digital document;
creating a hash of the associated data; asymmetrically
encrypting the hash with a private key to generate a digital
signature; encoding in a machine-readable code the digital
5 signature and the associated data; and recording the machine-
readable code onto a resulting hardcopy. The authenticity of
a printed hardcopy of the digital document can be verified
through comparison of data extracted from the printed
hardcopy with the associated data decoded and verified from
10 the machine-readable code.

The problems of counterfeiting and tampering
digital files are well known, serious, and growing. The
example of falsifying data marked on an original digital
15 document such as a digital identity document or a digital
version of a diploma is well known, and the concern is even
worse if considering a digital copy of the original (possibly
genuine) digital document. Simply keeping track of
identifiers such as serial numbers, or even including some
20 digital watermarks, is in general a weak response, because
counterfeiters can easily copy such numbers or digital
watermarks as well.

One other drawback of most conventional methods
25 for insuring the authenticity of digital files, or securing
their digital data, is that they tend to view files in
isolation, even if they are members of a well-defined group
such as a batch of digital documents for example. This
ignores valuable authenticating information.

30

It is therefore an object of the invention to
secure a printable digital file against forgery and

CLAIMS

1. Method of securing a given original digital file (A_1 ,
5 ..., A_8) belonging to a batch of a plurality of original
digital files (A_1 , ..., A_8) against forgery or tampering,
each original digital file (A_1 , ..., A_8) including its own
digital data (D_1 , ..., D_8), comprising the steps of:

for each original digital file (A_1 , ..., A_8) of the
10 batch, calculating by means of a one-way function (H) an
associated digital file signature (x_1 , ..., x_8) of its
digital data (D_1 , ..., D_8);

forming a tree based on the plurality of calculated
digital file signatures (x_1 , ..., x_8) for the original
15 digital files (A_1 , ..., A_8) of the batch and comprising nodes
arranged according to a given nodes ordering in the tree,
said tree comprising node levels from the leaf nodes,
corresponding to the plurality of digital file signatures
(x_1 , ..., x_8) respectively associated to the plurality of
20 original digital files (A_1 , ..., A_8) in the batch, to the
root node of the tree, every non-leaf node of the tree
corresponding to a digital signature by means of the one-way
function of a concatenation of the respective digital
signatures of its child nodes according to a tree
25 concatenation ordering, the root node corresponding to a
reference root digital signature (R), i.e. a digital
signature by means of the one-way function of a concatenation
of the digital signatures of the nodes of a penultimate nodes
level in the tree according to said tree concatenation
30 ordering;

associating with the given original digital file (A_1 ,
..., A_8) a corresponding digital verification key (k_1 , ...,

k_8) being a sequence of the respective digital signatures, from the leaf nodes level to the penultimate nodes level, of every other leaf node

having the same parent node in the tree that the leaf-node corresponding to the digital file signature $(x_1, \dots, x_8)$ of the given original digital file $(A_1, \dots, A_8)$, and successively at each next level in the tree, of every non-leaf node having the same parent node in the tree that the previous same parent node considered at the preceding level;

making available to a user the reference root digital signature (R) of the tree; and characterized by

including in the given original digital file $(A_1, \dots, A_8)$ a corresponding machine readable digital security marking (110) comprising a representation of its digital data $(D_1, \dots, D_8)$ and its corresponding digital verification key $(k_1, \dots, k_8)$,

thereby obtaining a marked original digital file $(A_1, \dots, A_8)$ of which digital data $(D_1, \dots, D_8)$ are secured against forgery or tampering.

2. Method according to claim 1, wherein the reference root digital signature (R) of the root node of the tree is either published in a media accessible to the user, or stored in a searchable root database accessible to the user, or stored in a blockchain, or in a database secured by a blockchain, accessible to the user.

3. Method according to claim 1 or claim 2, wherein

5 a virtual digital file is counted as belonging to the batch of original digital files ($A_1, \dots, A_8$), said virtual digital file including its own virtual digital data, and an associated virtual digital file signature obtained by means of the one-way function (H) of the virtual digital data, said virtual digital file being not real but only used for generating the associated virtual digital file signature from
10 its virtual digital data; and

the reference root digital signature (R) associated with said batch of original digital files ($A_1, \dots, A_8$) being calculated from a tree having all the digital files signatures of the original digital files ($A_1, \dots, A_8$) of the
15 batch, including the virtual digital file signature, as leaf nodes.

4. Method according to any one of claims 1 to 3, wherein

20 additional digital data ($D_1, \dots, D_8$) associated with the marked original digital file ($A_1, \dots, A_8$) are stored in a searchable information database accessible to the user via an information database interface operable to receive from the user an information

request containing digital data $(D_1, \dots, D_8)$, or a digital file signature $(x_1, \dots, x_8)$, obtained from a digital security

marking (110) of a marked original digital file ($A_1, \dots, A_8$), and send back corresponding additional digital data.

5. Method according to any one of claims 1 to 4, wherein the digital data ($D_1, \dots, D_8$) of the marked original digital file ($A_1, \dots, A_8$) include reference characteristic digital data of a corresponding unique physical characteristic of an associated object or individual.

6. Method according to any one of claims 1 to 5, wherein the digital data ($D_1, \dots, D_8$) of the respective original digital files ($A_1, \dots, A_8$) of the batch are spread between given fields common to all the digital files of the batch, and specific digital data relating to these fields are not included in the digital data ($D_1, \dots, D_8$) but clustered in a separate fields data block associated with the batch, and wherein:

i) the digital file signature ($x_1, \dots, x_8$) of an original digital file ($A_1, \dots, A_8$) is calculated with the one-way function of a concatenation of the corresponding digital data ($D_1, \dots, D_8$) and the fields data block; and
ii) the reference root digital signature (R) is made available to the user together with the associated fields data block.

7. Method of verifying the authenticity of a digital file secured according to the method of any one of claims 1 to 5,

or the conformity of a copy of such secured digital file with respect to the original one, characterized by comprising the steps of, upon processing a test file being said digital file

or said copy of the digital file by means of a processing unit connected to a memory:

having stored in the memory the test file;

reading a representation of digital data ($D_1, \dots, D_8$)

5 and of a digital verification key ($k_1, \dots, k_8$) on a digital security marking (110) of the stored test file, and extracting respectively corresponding test digital data and test digital verification key from said read representation;

10 having stored in the memory a reference root digital signature (R) of a root node of a tree of the batch of original digital files ($A_1, \dots, A_8$), and having programmed in the processing unit the one-way function (H) to calculate a digital signature of digital data ($D_1, \dots, D_8$) and of a concatenation of digital signatures according to the nodes
15 ordering in the tree and the tree concatenation ordering;

verifying whether the extracted test digital data and associated test digital verification key indeed correspond to the stored reference root digital signature (R) by performing the steps of:

20 calculating with the one-way function a test digital signature of the extracted test digital data, said test digital signature corresponding to a test leaf node in a test tree corresponding to the digital security marking (110) of the test file;

25 extracting from the sequence of digital signatures in the test digital verification key, a digital signature of every other leaf node of the test tree having the same parent node than that of the test leaf node and calculating a digital signature of a concatenation of the
30 test digital signature and the extracted digital signature of said every other leaf node, thus obtaining a digital signature of said same parent node of the test leaf node;

successively at each next level in the test tree and up to the penultimate nodes level, extracting from the sequence of digital signatures in the test digital verification key, a digital signature of every other non-leaf node of the test tree having the same parent node than that of the previous same parent node considered at the preceding step and calculating a digital signature of a concatenation of the digital signature of said respective every other non-leaf node and the obtained digital signature of said previous same parent node, thus obtaining a digital signature of said same parent node of said previous same parent node;

calculating a digital signature of a concatenation of the obtained digital signatures of the non-leaf nodes corresponding to the penultimate nodes level of the test tree, thus obtaining a candidate root digital signature of the root node of the test tree; and

checking whether the obtained candidate root digital signature matches the stored reference root digital signature (R),

whereby, in case said root digital signatures match, the digital data ($D_1, \dots, D_8$) of the test file are that of a genuine digital file.

8. Method according to claim 7, wherein the marked original digital file ($A_1, \dots, A_8$) is secured according to the method of claim 6, the memory of the processing unit further storing the associated fields data block, and wherein:

the step of calculating a test digital signature corresponding to a test leaf node in a test tree corresponding to the digital security marking (110) on the test file comprises calculating with the one-way function a

digital signature of a concatenation of the extracted test digital data and the stored fields data block.

9. Method according to any one of claims 7 and 8, wherein
5 the digital file is secured by storing the reference root digital signature (R) in a searchable root database accessible to the user according to the method of claim 2, and the processing unit is further connected to a communication unit operable to send and receive back data via
10 a communication link, comprising the preliminary steps of:
 sending with the communication unit via the communication link a request to said root database, and receiving back the reference root digital signature (R); and
 storing the received root digital signature in the memory
15 of the memory.

10. Method according to any one of claims 7 to 9, wherein the digital file is secured according to the method of claim 4,

and the imager is further equipped with communication means operable to send to the information database interface an information request containing digital data ($D_1, \dots, D_8$), or a digital file signature ($x_1, \dots, x_8$), obtained from the digital security marking (110) of the test file, and receive back corresponding additional digital data.

11. Method according to any one of claims 7 to 10, wherein the imager is further equipped with a sensor operable to detect a unique physical characteristic of respectively an associated object or individual, and the processing unit is programmed to extract corresponding characteristic digital data from a detection signal received from the sensor, the imager having stored in the memory reference characteristic digital data CDD corresponding to said unique physical characteristic of respectively the associated object or individual, comprising the further steps of, upon viewing a subject being said associated object or individual:

detecting with the sensor a unique physical characteristic of the subject and extracting corresponding candidate characteristic digital data CDD^c ;

comparing the obtained candidate characteristic digital data CDD^c with the stored reference characteristic digital data CDD; and

in case the candidate characteristic digital data CDD^c is similar to the stored reference characteristic digital data CDD, within a given tolerance criterion, the subject is considered as corresponding respectively to a genuine object or individual validly associated with a genuine digital file.

12. Digital file belonging to a batch of a plurality of original digital files ($A_1, \dots, A_8$) and secured according to the method of any one of claims 1 to 6, each original digital file ($A_1, \dots, A_8$) of the batch having its own digital data
5 ($D_1, \dots, D_8$) and corresponding digital verification key ($k_1, \dots, k_8$), said batch having a corresponding reference root digital signature (R), comprising:

10 a machine readable security marking including a representation of its digital data ($D_1, \dots, D_8$) and its verification key.

13. System for verifying the authenticity of a digital file, or the conformity of a copy of such digital file, with respect to a marked original digital file ($A_1, \dots, A_8$)
15 belonging to a batch of original digital files ($A_1, \dots, A_8$) secured according to the method of any one of claims 1 to 5, comprising an imager having an imaging unit, a processing unit with a memory, and an image processing unit, the memory storing a reference root digital signature (R) of a tree
20 corresponding to the batch of original digital files ($A_1, \dots, A_8$), and the one-way function (H) to calculate a digital signature of digital data ($D_1, \dots, D_8$) and of a

concatenation of digital signatures according to the nodes ordering of the tree and the tree concatenation ordering being programmed in the processing unit, said system being operable to:

have stored in the memory a test file being said digital file or said copy of the digital file;

read a representation of digital data ($D_1, \dots, D_8$) and of a digital verification key ($k_1, \dots, k_8$) on a digital security marking (110) of the stored test file, and extract
5 respectively corresponding test digital data and test digital verification key from said read representation;

verify whether the extracted test digital data and test digital verification key indeed correspond to the stored
10 reference root digital signature (R) by performing on the processing unit the programmed operations of:

calculating with the one-way function a test digital signature of the extracted test digital data, said test digital signature corresponding to a test leaf node in a
15 test tree corresponding to the digital security marking (110) of the test file;

extracting from the sequence of digital signatures in the test digital verification key, a digital signature of every other leaf node of the test tree having the same
20 parent node than that of the test leaf node and calculating a digital signature of a concatenation of the test digital signature and the extracted digital signature of said every other leaf node, thus obtaining a digital signature of said same parent node of the test
25 leaf node;

successively at each next level in the test tree and up to the penultimate nodes level, extracting from the sequence of digital signatures in the test digital verification key, a digital signature of every other non-
30 leaf node of the test tree having the same parent node than that of the previous same parent node considered at the preceding step and calculating a digital signature of a concatenation of the digital signature of said

respective every other non-leaf node and the obtained digital signature of said previous same parent node, thus obtaining a digital signature of said same parent node of said previous same parent node;

5 calculating a digital signature of a concatenation of the obtained digital signatures of the non-leaf nodes corresponding to the penultimate nodes level of the test tree, thus obtaining a candidate root digital signature of the root node of the test tree; and

10 checking whether the obtained candidate root digital signature matches the stored reference root digital signature (R),

 whereby, in case said root digital signatures match, the system is configured to deliver an indication that
15 the digital data of the test file are that of a genuine digital file.

14. System according to claim 13, wherein the marked original digital file ($A_1, \dots, A_8$) is secured according to
20 the method of claim 6, the memory of the processing unit further storing the associated fields data block, and wherein:

 the programmed operations of calculating a test digital signature corresponding to a test leaf node in a test tree
25 corresponding to the digital security marking (110) of the test file comprise calculating with the one-way function a digital signature of a concatenation of the extracted test digital data and the stored fields data block.

15. System according to any one of claims 13 and 14, wherein the marked original digital file ($A_1, \dots, A_8$) belongs to a batch of original digital files ($A_1, \dots, A_8$) secured according to the method of claim 5,

the system being further equipped with a sensor connected to the processing unit and operable to

detect a unique physical characteristic of an associated object or individual, and the processing unit being programmed to extract corresponding characteristic digital data from a detection signal received from the sensor, the system having stored in the memory reference characteristic digital data CDD corresponding to said unique physical characteristic of the associated object or individual, the system being further operable to:

detect with the sensor a unique physical characteristic of a subject being said associated object or individual, and extract corresponding candidate characteristic digital data CDD^c;

compare the obtained candidate characteristic digital data CDD^c with the stored reference characteristic digital data CDD; and

in case the candidate characteristic digital data CDD^c is similar to the stored reference characteristic digital data CDD, within a given tolerance criterion, deliver an indication that the subject is considered as genuine.