

CLAIMS

1. Method of securing a given original digital file of a batch of a plurality of original digital files (A_1, A_2, A_3) against forgery or tampering, each original digital file of the batch containing its own digital data (D_1, D_2, D_3), characterized by comprising the steps of:

for each original digital file of the batch, calculating by means of a one-way function an associated digital file signature (x_1, x_2, x_3) of its digital data;

calculating a reference aggregated digital signature (B) corresponding to the batch of original digital files from all the digital file signatures of the original digital files of the batch by means of a one-way accumulator of said digital file signatures, and making available to a user the reference aggregated digital signature;

determining a digital file verification key (k_i) corresponding to the digital file signature of said given original digital file by means of a partial one-way accumulator of all the other digital file signatures used for calculating the reference aggregated digital signature, whereby a candidate digital file signature corresponds to that of an original digital file of the batch only if the reference aggregated digital signature is calculated by means of the one-way function of said candidate digital file digital data and corresponding digital file verification key; and

including in the given original digital file a digital representation of a machine readable security marking (110) containing a representation of the digital data of the given original digital file and its corresponding digital file verification key, both included into the machine readable security marking via encoding,

thereby obtaining a marked original digital file of which digital data are secured against forgery or tampering.

2. Method according to claim 1, wherein the reference aggregated digital signature associated with the batch of original digital files is either published in a media accessible to the user, or stored in a searchable aggregated signature database

accessible to the user, or stored in a blockchain (260), or in a database secured by a blockchain, accessible to the user.

3. Method according to claim 2, wherein the marked original digital file further includes aggregated signature access data containing information sufficient to access to the reference aggregated digital signature corresponding to the batch of original digital files, said information being a link to an aggregated signature acquisition interface of, respectively, one of the following:

- the media wherein the reference aggregated digital signature is published, the media being accessible to the user via said aggregated signature acquisition interface operable to receive from the user an aggregated signature request containing digital data, or a digital signature of said digital data, obtained from the digital representation of a machine readable security marking of a marked original digital file, and send back a reference aggregated digital signature of associated batch;
- the searchable aggregated signature database wherein the reference aggregated digital signature is stored, the aggregated signature database being accessible to the user via said aggregated signature acquisition interface operable to receive from the user an aggregated signature request containing digital data, or a digital signature of said digital data, obtained from the digital representation of a machine readable security marking of a marked original digital file, and send back a reference aggregated digital signature of associated batch;
- the blockchain, respectively the database secured by the blockchain, wherein the time-stamped aggregated digital signature is stored, the blockchain, respectively the database secured by the blockchain, being accessible to the user via said aggregated signature acquisition interface operable to receive from the user an aggregated signature request containing digital data, or a digital signature of said digital data, obtained from the digital representation of a machine readable security marking of a marked original digital file, and send back a reference aggregated digital signature of associated batch.

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

a virtual digital file (A_v) is counted as belonging to the batch of original digital files, said virtual digital file having corresponding virtual digital data (D_v), and an associated virtual digital file signature (x_v) obtained by means of the one-way

function of its virtual digital data, said virtual digital file being not real but only used for generating the associated virtual digital file signature from the corresponding virtual digital data; and

the reference aggregated digital signature associated with said batch of original digital files being calculated from all the digital file signatures of the original digital files of the batch, including the virtual digital file signature, by means of the one-way accumulator.

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

the one-way function is a hash function (H) and a digital file signature of an original digital file is a sequence of a given plurality of bits of lower weights selected from the bits of a hash value of the corresponding digital data.

6. Method according to any one of claims 1 to 5, wherein

additional digital data corresponding to the digital data associated with the marked original digital file are stored in a searchable information database (250) accessible to the user via an information database interface operable to receive from the user an information request containing digital data, or corresponding digital file signature data, obtained from the digital representation of a machine readable security marking of a marked original digital file, and send back corresponding additional digital data.

7. Method according to any one of claims 1 to 6, wherein the digital data of the marked original digital file include reference characteristic digital data CDD (230e) of a corresponding unique physical characteristic of an associated object or individual.

8. Method of verifying the authenticity of a digital file secured according to the method of any one of claims 1 to 7, 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 and of a test file verification key on a digital representation of a machine readable security marking in the stored test file, and extracting respectively corresponding digital data and test file verification key from said read representation;

having stored in the memory a reference aggregated digital signature of a corresponding batch of digital files, and having programmed in the processing unit the one-way function and the one-way accumulator;

verifying that the extracted digital data and test file verification key indeed correspond to the stored reference aggregated digital signature by performing the steps of:

calculating a digital signature of the extracted digital data with the one-way function;

calculating a candidate aggregated digital signature from the calculated digital signature of the extracted digital data and the extracted test file verification key with the one-way accumulator; and

checking that the obtained candidate aggregated digital signature matches the stored reference aggregated digital signature,

whereby, in case said aggregated digital signatures match, the digital data of the test file are that of a genuine original digital file.

9. Method according to claim 8, wherein the digital file is secured by storing the reference aggregated digital signature associated with batch of original digital files in a searchable aggregated signature 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 a communication link, comprising the preliminary steps of:

sending with the communication unit via the communication link a request to said aggregated signature database, and receiving back the reference aggregated digital signature associated with batch of original digital files; and

storing the received aggregated digital signature in the memory.

10. Method according to claim 8, wherein the digital file is secured according to the method of claim 3 and the processing unit is further connected to a communication unit operable to send and receive back data via a communication link, comprising the preliminary steps of:

reading the aggregated signature access data included in the test file;

sending with the communication unit via the communication link an aggregated signature request to said aggregated signature acquisition interface containing the digital data, or a digital signature of said digital data, obtained from the digital representation of a machine readable security marking in the test file, and receiving back a corresponding reference aggregated digital signature of associated batch; and

storing the received aggregated digital signature in the memory.

11. Method according to any one of claims 8 to 10, wherein the digital file is secured according to the method of claim 6 and the processing unit is further connected to communication means operable to send to the information database interface an information request containing digital data, or corresponding digital file signature, obtained from the digital representation of a machine readable security marking in the test file, and receive back corresponding additional digital data.

12. Method according to any one of claims 8 to 11, wherein the digital file is secured according to the method of claim 7 and the processing unit is connected to a sensor operable to detect a unique physical characteristic of an associated object or individual, the processing unit being programmed to extract corresponding unique physical characteristic digital data from a detection signal received from the sensor, the processing unit having stored in the memory reference characteristic digital data CDD corresponding to said unique physical characteristic of the associated object or individual, comprising the further steps of, upon viewing a subject being, respectively, said associated object or individual:

detecting a unique 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 genuine.

13. Marked digital file belonging to a batch of a plurality of original digital files and secured against forgery or tampering according to the method of any one of claims 1 to 7, each original digital file of the batch having its own digital data, said batch having a corresponding reference aggregated digital signature, comprising:

a digital representation of a machine readable security marking including a representation of digital data of the marked digital file and a corresponding digital file verification key.

14. Marked digital file according to claim 13, wherein the digital data of the marked digital file include reference characteristic digital data CDD of a corresponding unique physical characteristic of an associated object or individual.

15. Marked digital file according to claim 14, wherein the unique physical characteristic of the associated object is that of a material-based security marking applied on the associated object.

16. System for verifying the authenticity of a marked original digital file secured according to the method of any one of claims 1 to 7, or the conformity of a copy of such digital file with respect to the original one, comprising a processing unit with a memory, the memory storing a reference aggregated digital signature of a corresponding batch of digital files, and the one-way function and the one-way accumulator being programmed in the processing unit, operable to:

acquire a test file being said digital file or a copy of the digital file and store the acquired test file in the memory;

read a representation of digital data and of a test file verification key on a digital representation of a machine readable security marking in the stored test file, and extract respectively corresponding digital data and test file verification key from said read representation;

verify that the extracted digital data and test file verification key indeed correspond to the stored reference aggregated digital signature by executing the steps, programmed in the processing unit, of:

calculating a digital signature of the extracted digital data with the one-way function;

calculating a candidate aggregated digital signature from the calculated digital signature of the extracted digital data and the extracted test file verification key with the one-way accumulator; and

checking that the obtained candidate aggregated digital signature matches the stored reference aggregated digital signature,

whereby, in case said aggregated digital signatures match, the digital data of the test file are that of a genuine original digital file and the system is operable to deliver an indication that the digital data on the test file is that of a genuine original digital file.

17. System according to claim 16, for verifying a digital file secured according to the method of claim 7, or the conformity of a copy of such digital file with respect to the original one, 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 is 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.