

CLAIMS

1. A method of automatic object recognition, comprising:
receiving object data representing one or more discriminating characteristics
5 of a physical object or group of physical objects;
processing the object data by means of a machine-learning-based object
recognition process to obtain discriminating data representing one or more
collision resistant virtual representations of the physical object or group of
physical objects;
10 comparing at least one of the discriminating data and an original hash value
derived therefrom by application of a pre-determined cryptographic hash
function thereto with corresponding reference data stored in one or more da-
ta repositories with restricted access;
If said comparison with the reference data results in a match, outputting digi-
15 tally signed identification data comprising said hash value.
2. A method of training a system for automatic object recognition, the method
comprising:
receiving object data representing one or more discriminating characteristics
20 of a physical object or group of physical objects;
processing the object data by means of a machine-learning-based object
recognition process to obtain original discriminating data representing one or
more collision resistant virtual representations of the physical object or group
of physical objects;
25 storing reference data comprising the original discriminating data and an
original hash value derived therefrom by application of a pre-determined
cryptographic hash function thereto into one or more data repositories with
restricted access.
- 30 3. The Method of claim 2, wherein storing the reference data comprises storing
the original discriminating data into a first one of the data repositories and
storing identification data comprising the original hash value into a separate
second one of the data repositories such that neither the first nor the second
35 data repository stores both the original discriminating data and the corre-
sponding original hash value.

4. The method of claim 2 or 3, wherein processing the object data to obtain said original discriminating data comprises generating, by means of performing one or more predefined modification operations, a plurality of collision resistant virtual representations of said physical object or group of physical objects, such that at least two of these virtual representations represent the same physical object or group of physical objects, but each at a different condition.
5. The method of any one of claims 2 to 4, wherein storing the reference data comprises storing combined data, which is formed as a combination of the reference data and an additional adjunct value, which is defined independent from said reference data, into the one or more data repositories with restricted access.
6. The method of any one claims 2 to 5, further comprising iteratively re-training the system for automatic object authentication based on additional object data representing discriminating characteristics of a physical object or group of physical objects, for which respective original reference data has already been previously generated and stored in the one or more data repositories during a previous iteration step of training the system, wherein the additional object data serves as input data for said machine-learning-based object recognition process.
7. The method of any one claims 2 to 6, wherein storing the reference data comprises one or more of the following steps:
storing the reference data in a digitally signed form into at least one of said data repositories;
storing or causing one or more nodes of a blockchain environment to store the identification data in a digitally signed form into a block of a blockchain related to said blockchain environment;
storing or causing one or more nodes of a blockless distributed ledger environment to store the identification data in a digitally signed form into at least one node of said blockless distributed ledger environment;
storing the identification data in a digitally signed form into a storage of a Public/Private-Key environment.

- 8 The method of any one of the preceding claims, wherein, the method is performed by a system comprising two or more separate devices, which collectively perform the method, and which are communicatively connected to each other by one or more data links being protected against unauthorized interception.
- 5
9. A system for automatic object recognition, the system being configured to perform the method of one or more of the preceding claims.
- 10 10. A computer program comprising instructions, which when executed on one or more processors of a system for automatic object recognition according to claim 9 causes the system to perform the method according to any one of claims 1 to 8.
- 15 11. A method of authenticating an object with an object authentication device, comprising:
sensor-based detecting of one or more discriminating characteristics of a physical object or group of physical objects;
generating object data representing said one or more discriminating characteristics of said physical object or group of physical objects;
20 communicating said object data to a system according to claim 9;
receiving digitally signed identification data from said system in response to said communicating of said object data;
reading a marking provided on or in combination with the physical object or group of physical objects, respectively, to obtain therefrom digitally signed identity information;
25 verifying the correctness of each of the digital signature of the identification data and the digital signature of the identity information;
comparing the received identification data with the obtained identity information to verify the authenticity of said object or group of objects based on the result of this comparison; and
30 outputting authentication information indicating whether, according to the result of this verification, said physical object or group of physical objects was determined to be authentic.
- 35

12. The method of claim 11, wherein said sensor-based detecting of one or more discriminating characteristics of the physical object or group of physical objects comprises detecting at least one discriminating characteristic that is, at least substantially, invariant under variations of the environmental conditions at which said at least one discriminating characteristic is being detected.
13. The method of claim 11 or 12, further comprising:
including the original hash value or another object-specific information contained in the identification data into the output authentication information.
14. The method of claim 13, further comprising a storing process, wherein the storing process comprises digitally signing and storing or causing another device to store said original hash value or said other object-specific information in the digitally signed form into a block of a first blockchain or a node of a first blockless distributed ledger.
15. The method of claim 14, wherein in the storage process further comprises:
reading a marking provided on or in connection with the physical object or group of objects to be authenticated or detecting one or more selected properties of said object or group of objects to obtain supplementary information relating thereto; and
digitally signing and storing or causing another device to store said supplementary information in the digitally signed form into a block of second blockchain being separate from the first blockchain or into a node of a second blockless distributed ledger being separate from the first blockless distributed ledger.
16. The method of any one of claims 11 to 15, further comprising one or more of the following:
performing a user authentication and allowing or denying the user to perform an object authentication with said object authentication device based on the result of the user authentication;
communicating the authentication information and/or the identification data, in whole or part, and/or further information derived therefrom, over a communication link to an opposing side;

capturing and sending security-related information over a communication link to an opposing side;
detecting a security event in information contained in a signal received from the opposing side over the communication link.

5

17. The method of any one of claims 11 to 16, further comprising sensor-based detecting of one or more of the following as a security event:

- an attempt or actual act of physical intrusion into the object authentication device;
- 10 – an attempt or actual act of locally or remotely accessing an internal control functionality of the object authentication device, wherein such access is not available to a user of the object authentication device in the course of its normal operation.

15 18. The method of any one of 11 to 17, further comprising performing one or more of the following security measures in reaction to detection of a security event:

- locking the object authentication device such as to limit or prevent its further use;
- 20 – self-destroying at least one functional part of the object authentication device or destroying data stored therein in order to prevent its further use or access by a user;
- outputting an error message.

25 19. An object authentication device being adapted to perform the method of any one of claims 11 to 18.

20. A computer program comprising instructions, which when executed on one or more processors of an object authentication device according to claim 19
30 causes the object authentication device to perform the method according to any one of claims 11 to 18.

21. A system for automatic object authentication, comprising the system for automatic object recognition of claim 9 and an object authentication device of
35 claim 19, the system of claim 9 and the device of claim 19 being configured

to collectively recognize and authenticate a physical object or group of physical objects.