(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2018 (28.06.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/113803 A1

(51) International Patent Classification:
G06K 9/00 (2006.01) *G06K 9/22* (2006.01) *G06K 9/18* (2006.01)

(21) International Application Number:
PCT/CZ2017/050062

(22) International Filing Date:
20 December 2017 (20.12.2017)

(25) Filing Language: Czech

(26) Publication Language: English

(30) Priority Data:
PV 2016-832 23 December 2016 (23.12.2016) CZ

(71) Applicant: **ADUCID S.R.O.** [CZ/CZ]; Videnska 204/125, 61900 Brno - Prizrenice (CZ).

(72) Inventors: **NEUMANN, Libor**; Brdickova 1910/23, 15500 Praha 5 - Luziny (CZ). **RIHAK, Miroslav**; Terasova 3063/60, 61600 Brno - Zabovresky (CZ).

(74) Agent: **HARTVICHOVA, Katerina**; HARBER IP s.r.o., Na Belidle 3, 15000 Praha 5 (CZ).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

WO 2018/113803 A1

(54) Title: MULTI-FACTOR AUTHENTICATION METHOD

(57) Abstract: The present invention provides a method of authenticating a user and/or a mobile device by means of an authentication image and a mobile authentication device provided with a display and at least two cameras located on mutually opposite sides of the mobile device, the authentication image being scanned by a first camera of the mobile device, located opposite the mobile device display, and simultaneously scanning the biometric authentication factor from the user's head and/or body by a second camera of the mobile device, located on the mobile device display side; the data thus obtained are then evaluated and, if the evaluation result is positive, the user and/or the mobile device are authenticated.

Multi-factor Authentication Method

Technical Field

The present invention relates to multi-factor authentication of a user and/or a mobile authentication device, wherein the use of a mobile telephone as the authentication device is particularly preferred.

Background Art

Multiple factors are used for strong authentication. For example, an authentication object (such as a smart card, an authentication calculator, a mobile device equipped with a suitable software) and a biometric factor scanned by a specialized device (e.g., a fingerprint reader). Secret information entered by the user (such as PIN, password, touch screen pattern), or otherwise acquired from the environment is commonly used as a second factor. This information entered by the user or otherwise acquired from the environment is called the second factor.

Commonly commercially available specialized authentication objects must be equipped with specialized technical means for scanning or inputting the second factor, and the user must manipulate them properly to enter the second factor.

There are authentication solutions that scan an image, such as a QR code, with a built-in camera. The user takes his mobile device and points its camera to the authentication image to be scanned. The authentication software then recognizes the image and initiates the authentication process.

The currently commercially available mobile devices, such as phones or tablets, are equipped with two cameras, one camera being located on the side of the display (a so-called "selfie" camera), and the other camera being located on the opposite side of the device. Some devices also feature stereo cameras.

Summary of the Invention

The present invention provides a method for authenticating a user and/or a mobile device by means of an authentication image and of a mobile authentication device provided with a display and with at least two cameras located on mutually opposite sides of the mobile device, wherein the authentication image is scanned by a first camera of the mobile device located on a side which is opposite to the side comprising the mobile device display, and at the same time a biometric authentication factor from the head and/or body of the user is scanned/captured by a second camera of the mobile device located on the side comprising the mobile device display; the thus obtained data are then evaluated and, if the evaluation result is positive, the user and/or the mobile device are authenticated.

The authentication image is an image destined for machine reading, such as a barcode, a QR code. For example, the authentication image may be placed on a document or an object, or displayed on an electronic device display (e.g., a computer, a tablet, a mobile phone). The authentication image for displaying on an electronic device display can be obtained, for example, by generating an image by a target application or by another computer program.

When scanning the authentication image, the user takes his mobile device and points its first camera to the authentication image to be scanned. Authentication software in the mobile device recognizes the image and initiates the authentication process. Softwares for scanning a machine-readable image, such as a QR code, usually display the image, which is being scanned, on the mobile device display, and the user visually checks on the display the correct location of the authentication image before and during scanning. This visual check is naturally performed by the user at roughly the same position of the body, head, face, eyes to the display and to the camera, respectively, to the entire device, while being in the field of vision of the second camera located on the side of the mobile device display.

The biometric authentication factor can be any biometric characteristic that can be scanned from the head and/or body of the user, in particular from the face or eyes of the user. When this biometric authentication characteristic is scanned together (at the same time) with scanning the authentication image, the present invention benefits from the fact that the user automatically assumes the same position of the body, the head, and parts thereof, such as the face and/or eyes while scanning the authentication image and checking its image and/or location on the mobile device display, and the user is in the field of vision of the second camera located on the side of the display. Thus, the user does not have to focus or force himself to assume a special position to scan the biometric authentication factor. Scanning a biometric authentication factor is thus reproducible and does not require any separate step, nor does it put an unnecessary burden on the user.

Preferably, the authentication mobile device is a mobile phone or a tablet. A vast majority of commercially available mobile phones and tablets are currently provided with two cameras suitable for performing the method of the invention.

The biometric authentication factor and the authentication image can be scanned independently from each other in any suitable electromagnetic radiation wavelength range, i.e. visible light range, or invisible radiation such as IR, UV radiation. Commercially available are also mobile devices equipped with stereo cameras for 3D image scanning. These cameras can also be advantageously used to scan both the biometric authentication factor and the authentication image.

The advantages of the present invention include the fact that commonly available mobile devices can be used as authentication devices. Therefore, the user does not need to purchase any especially dedicated single-use biometric factor scanning devices. The user's activity in scanning both factors at the same time is natural; the method prevents unnecessary burdening of the user during the scanning of the biometric factor and does not impose any additional requirements on the user. Furthermore, the security of authentication is increased, and the potential attacker is in a more complicated situation than when any other way of scanning biometric data is used for authentication.

It will be apparent to those skilled in the art that this method can be combined with the use of other authentication factors.

It will be appreciated by those skilled in the art that other technical equipment in addition to the second camera may be used for scanning the biometric characteristics of the user.

The authentication image and the biometric factor, and optionally other authenticated factors scanned or inputted, are evaluated for authentication purposes by known methods.

If the result of the evaluation is positive, the user is authenticated, i.e., it is confirmed that it is the authorized mobile device and that an authorized person operates the mobile device.

A positive result of evaluation can typically include: compliance with predetermined reference values, or a positive result of a cryptographic operation such as verification of electronic signature value, or a predetermined minimum compliance with predefined reference values, or a positive result of evaluation of various partial positive evaluations.

In one preferred embodiment of the invention, the authentication mobile device processes the biometric authentication factor data (e.g., the image of the head, face, eyes, or other part of the head, body, or a part thereof), and evaluates the processed data. The authentication mobile device then transmits the result of the evaluation to the authentication server. This can be done using known algorithms and methods of evaluation of biometric data.

In one preferred embodiment of the invention, the authentication mobile device transmits the scanned image of the head, face, eyes, or other parts of the head, body, or a part thereof, carrying the biometric information, for processing to the authentication server as part of the authentication process. The authentication server then evaluates the scanned image, using known algorithms and methods of evaluation of biometric data.

In another preferred embodiment of the invention, the authentication mobile device processes the scanned image of the head, face, eyes, or other parts of the head, body, or a part thereof, carrying the biometric information, and performs a numerical transformation of the scanned image into a set of derived data, so-called descriptors. Known algorithms and methods of transforming biometric data may be used for the transformation. The computed descriptors are then transmitted by the authentication mobile device for evaluation to the authentication server as part of the authentication process.

In yet another preferred embodiment of the invention, the authentication mobile device processes the scanned image of the head, face, eyes, or other parts of the head, body or a part thereof, carrying biometric information, and performs numerical transformation of the scanned image into a set of descriptors. Known algorithms and methods of transforming biometric data may be used for the transformation. The authentication mobile device then modifies the computed descriptors by a pseudo-random authenticated shared secret and transmits the data resulting from the modification to the authentication server as part of the authentication process. The authentication server then uses the authenticated shared secret for evaluation of the descriptors.

In still another preferred embodiment of the invention, the authentication mobile device processes the scanned image of the head, face, eyes or other parts of the head, body, or a part thereof, carrying biometric information, by means of a parametric transformation using a pseudo-random authenticated shared secret, and transmits the result of the transformation for processing to the authentication server as part of the authentication process. The authentication server reconstructs the scanned image by means of inverse parametric transformation using the pseudo-random authenticated shared secret, and evaluates the scanned image data. This can be done by known algorithms and methods of evaluation of biometric data.

In yet another preferred embodiment of the invention, the authentication mobile device evaluates the scanned image of the head, face, eyes or other parts of the head, body, or a part thereof, carrying biometric information (this can be done by known algorithms and methods of evaluation of biometric data), and transmits the result of the evaluation to the authentication server.

After authentication, the target application or service provider may allow the user, for example, to access data, perform secure operations, and/or transmit data by an authenticated channel.

The invention further includes a data processing device comprising means for carrying out the steps of the method of the invention.

The invention further includes a computer program product comprising instructions which, when the program is executed by a mobile authentication device and/or by an authentication server, cause the mobile authentication device and/or the authentication server to carry out the steps of the method of the invention.

Example of carrying out the invention

A user uses as the authentication device a mobile phone with a display and two cameras located on mutually opposite sides of the mobile phone. The authentication image is a QR code printed on a document. The user launches on the mobile phone an authentication application that uses the QR Code Reader application. The user then directs a first camera, located on the opposite side of the mobile device than the side on which the display is located, to the printed QR code. The QR Code Reader application displays on the mobile device display the QR code and a frame in which the QR code must be placed during scanning. At the same time, the authentication application uses a second camera, located on the same side of the mobile phone as the display, scans/captures the image of the user's face and reads or calculates biometric characteristics from the face image. During this process, the user naturally assumes the same face position to the mobile phone, so the scanning of the biometric characteristics does not imply any additional burden or any additional procedure for the user. The data obtained by scanning the QR code and by scanning the biometric characteristics of the user's face are then evaluated by known means and, when the evaluation result is positive, the user and/or the mobile device is authenticated.

Industrial applicability

The present invention provides a method of multi-factor authentication of a user and/or a mobile authentication device, usable in particular when a mobile phone is used as the authentication means (or electronic identification means). After a successful authentication by means of the mobile phone, the application or service provider may allow the user, for example, to access data, perform secure operations, and/or transmit data by an authenticated channel.

CLAIMS

1. A method of authentication by means of an authentication picture and a mobile authentication device equipped with a display and at least two cameras located on mutually opposite sides of the mobile device, wherein

- an authentication image is scanned by a first camera of the mobile device, said first camera being located on a side of the mobile device which is opposite to the side comprising the mobile device display, and simultaneously
- scanning a biometric authentication factor from the head and/or body of the user by a second camera of the mobile device, said second camera being located on the same side as the mobile device display;
- the data thus obtained are then evaluated and, when the evaluation result is positive, the user and/or the mobile device is authenticated.

2. The method according to claim 1, wherein the authentication image is selected from the group consisting of an image, a barcode, a QR code.

3. The method according to claim 1 or 2, wherein the biometric authentication factor is a biometric characteristic scanned from the head part, in particular from the face or the eyes.

4. The method according to any one of the preceding claims, wherein at least one of the cameras of the mobile authentication device is a stereo camera enabling 3D image scanning.

5. The method according to any one of the preceding claims, wherein the authentication image and/or the biometric authentication factor is scanned in the spectral range of light visible by human eye.

6. The method according to any one of claims 1 to 4, wherein the authentication image and/or the biometric authentication factor is scanned in the spectral range of radiation invisible by human eye.

7. The method according to any one of claims 1 to 6, wherein after scanning the authentication image and the biometric authentication factor, the mobile authentication device transmits the scanned image of the head and/or its part and/or body and/or its part, bearing the biometric information, to the authentication server for processing as part of the authentication process, and the authentication server then evaluates the scanned data.

8. The method according to any one of claims 1 to 6, wherein after scanning the authentication image and the biometric authentication factor, the mobile authentication device processes the scanned image of the head and/or its part and/or the body and/or its part, bearing the biometric information, by means of a numerical transformation of the scanned images into a set of descriptors, and the computed descriptors are then transmitted by the mobile authentication device to the authentication server for evaluation as part of the authentication process.

9. The method according to any one of claims 1 to 6, wherein after scanning the authentication image and the biometric authentication factor, the mobile authentication device processes the image of the head and/or its part and/or body and/or its parts, bearing the biometric information, and performs a numerical transformation of the scanned image into a set of descriptors, the computed descriptors are then modified by the mobile authentication device by a pseudo-random authenticated shared secret, and the modified descriptors are transmitted by the mobile authentication device to the to the authentication server as part of the authentication process, and the authentication server then uses the authenticated shared secret for evaluation of the descriptors.

10. The method according to any one of claims 1 to 6, wherein after scanning the authentication image and the biometric authentication factor, the mobile authentication device processes the scanned image of the head and/or its part and/or the body and/or its parts, bearing the biometric information, by means of parametric transformation using a pseudo-random authenticated shared secret and transmits the result for processing to the authentication server as part of the authentication process, and the authentication server, by means of inverse parametric transformation using the pseudo-random authenticated shared secret, reconstructs the scanned image and evaluates it.

11. The method according to any one of claims 1 to 6, wherein after scanning the authentication image and the biometric authentication factor, the authentication mobile device evaluates the scanned image of the head, face, eyes or other parts of the head, body, or a part thereof, carrying biometric information, and transmits the result of the evaluation to the authentication server.

12. A data processing device comprising means for carrying out the steps of the method of any one of claims 1 to 11.

13. A computer program product comprising instructions which, when the program is executed by a mobile authentication device and/or by an authentication server, cause the mobile authentication device and/or the authentication server to carry out the steps of the method of any one of claims 1 to 11.

INTERNATIONAL SEARCH REPORT

International application No
PCT/CZ2017/050062

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K9/00 G06K9/18 G06K9/22
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016/029853 A1 (TENCENT TECH SHENZHEN CO LTD [CN]) 3 March 2016 (2016-03-03) page 4, line 24 - page 4, line 29 page 5, line 11 - page 5, line 24 page 9, line 6 - page 9, line 27 page 10, line 18 - page 10, line 19 page 12, line 5 - page 12, line 9 page 21, line 24 - page 21, line 25 figures 2A, 4 & US 2017/161750 A1 (YAO LONGYANG [CN] ET AL) 8 June 2017 (2017-06-08) paragraphs [0046] - [0055], [0085] - [0098], [0108] - [0109], [0135] - [0137], [0212] figures 2A, 4 ----- -/--	1-13

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 23 April 2018	Date of mailing of the international search report 02/05/2018
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Bouganis, Alexandros

2

INTERNATIONAL SEARCH REPORT

International application No
PCT/CZ2017/050062

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2014/124014 A1 (VYNCA L L C [US]) 14 August 2014 (2014-08-14) paragraph [0007] - paragraph [0009] paragraph [0058] - paragraph [0060] paragraph [0095] - paragraph [0105] paragraph [0112] - paragraph [0113] paragraph [0124] -----	1-13
A	US 2016/119317 A1 (NEUMANN LIBOR [CZ]) 28 April 2016 (2016-04-28) paragraph [0015] - paragraph [0017] -----	9,10
A	S SUDHARSANAN: "Shared key encryption of JPEG color images", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 51, no. 4, 1 November 2005 (2005-11-01), pages 1204-1211, XP055469191, NEW YORK, NY, US ISSN: 0098-3063, DOI: 10.1109/TCE.2005.1561845 section II -----	9,10

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/CZ2017/050062

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016029853 A1	03-03-2016	CN 104184589 A	03-12-2014
		US 2017161750 A1	08-06-2017
		WO 2016029853 A1	03-03-2016
WO 2014124014 A1	14-08-2014	US 2015358400 A1	10-12-2015
		US 2016335479 A1	17-11-2016
		WO 2014124014 A1	14-08-2014
US 2016119317 A1	28-04-2016	BR 112015028638 A2	25-07-2017
		CN 105612728 A	25-05-2016
		EP 3000216 A1	30-03-2016
		JP 2016522637 A	28-07-2016
		KR 20160013135 A	03-02-2016
		RU 2015150542 A	27-06-2017
		US 2016119317 A1	28-04-2016
		WO 2014187436 A1	27-11-2014