

# **A SYSTEM SUITABLE FOR DETECTING AN IDENTIFICATION CARD, AND AN APPARATUS AND AN AUTHENTICATION METHOD IN ASSOCIATION THERETO**

## **5 Field Of Invention**

The present specification generally relates to a system suitable for detecting an identification card. The present specification further relates to one or both of an apparatus and an authentication method associable to the system.

## **10 Background**

In the electronic know your client/customer (eKYC) context, authentication can, for example, be by manner of verifying an identification (ID) card belonging to a client/customer.

15 This can conventionally be done by manner of, for example, prompting a client/customer to scan/capture an image of an ID card belonging to or associated with the client/customer, for the purpose of authentication.

One conventional solution/technique is to use an electronic device (e.g., a  
20 Smartphone) to capture an image of the ID card belonging to or associated with a client/customer. Upon verifying that the captured image indeed corresponds to the ID card of the client/customer, authentication can be completed.

The present specification contemplates that conventional solutions/techniques could  
25 possibly be subject to circumvention by one or more unauthorized parties/individuals (e.g., who are not true owners of the ID card(s) used for authentication). For example, an unauthorized individual may display a screenshot of a captured image (e.g., which may be obtained fraudulently) of an ID card on a high resolution monitor and such a high resolution screenshot may potentially be used for verification and  
30 subsequent successful completion of authentication. Therefore, reliability/integrity of authentication may be a concern/issue.

Moreover, conventional solutions/techniques may be reliant on Moiré pattern-based analysis of a captured image and/or boundary-based checks concerning a captured image for the purpose of verifying authenticity of a screenshot and/or a captured image of an ID card. The present contemplates that such verification techniques  
5 may require a large amount of data and large-scale training samples to train a classifier model, and hence may not be efficient.

The present specification contemplates that there is a need to improve the manner in which authentication can be done in a reliable and/or efficient manner.

10

### **Summary of the Invention**

To improve the manner in which authentication/verification can be performed (i.e., in a reliable and/or secure manner), the present specification contemplates route-based detection. Route-based detection can be based a set of detection points  
15 generated based on one or both of a predetermined-based manner and a random-based manner.

Generally, route-based detection can be associated with a set of detection points which can be displayed on the display of a device (e.g., a portable electronic device  
20 such as a Smartphone or a non-portable electronic device such as a kiosk station). Each detection point of the set of detection points can be associated with a location/position (i.e., as displayed on the display). As will be discussed later in further detail, the detection points can be displayed in a sequential manner or a simultaneous manner.

25

When authentication is initiated, a user can be prompted to capture an image of his/her ID card in a manner so that the captured image coincides with the location/position of a detection point as displayed on the display. For example, a set of detection points can be displayed on the display of the Smartphone (having an  
30 image capturing device such as a camera) used by the user. The user, holding the Smartphone, can position the Smartphone in a manner such that an image of the ID card is captured in a manner so as to coincide with the displayed detection point (i.e., as displayed on the display). This capturing process (i.e., the process of capturing

an image of the ID card) can be repeated in the same manner for each detection point of the set of detection points. Authentication can be successfully completed after an image of the ID card is captured in a manner so as to coincide with each displayed detection point of the set of detection points.

5

In accordance with an embodiment of the disclosure, there is provided an apparatus. The apparatus can include at least one display and at least one capturing device. The apparatus can further include at least one processor coupled to one or both of the at least one display and the at least one capturing device.

10

The apparatus can further include at least one memory device coupled to the processor. The memory device can carry a set of instructions that when executed:

15

- causes the at least one display to display a set of detection points, each detection point in the set of detection points being associable with a position on the display;

20

- causes the at least one capturing device to capture data associated with an Identification (ID) Card which is associated with a customer, captured data being associated with at least one image of the ID card; and

25

An image of the ID card can be captured so as to coincide with a corresponding detection point.

In accordance with another embodiment of the disclosure, there is provided an apparatus.

30

The apparatus can include a capturing device (e.g., a camera), a processor (e.g., a microprocessor) and a display (e.g., a screen), in accordance with an embodiment of

the disclosure. The capturing device and the display can, in one embodiment, be coupled to the processor.

The capturing device can capture data associated with an Identification (ID) Card.

- 5 The ID card can be associated with a customer. Moreover, captured data can be associated with at least one image of the ID card (i.e., at least one captured image of an ID card).

- 10 The processor can process the captured data in a manner so as to determine at one or both of location of each corner of the ID card and center of the ID card (i.e., location of each corner of the ID card and/or center of the ID card).

The display can display a set of detection points. Each detection point in the set of detection points can be associated with a position/location on the display.

- 15 Moreover, the apparatus can be controlled (e.g., by a customer) so that the capturing device can capture an image of the ID card in a manner so as to coincide (e.g., in terms of location/position) with a corresponding detection point. Successful authentication can, for example, be determined after all taken images of the ID card (i.e., captured images of the ID card) have been determined to coincide with the corresponding detection points.
- 20

In accordance with yet another embodiment of the disclosure, there is provided an authentication method.

- 25 The authentication method can include providing a set of detection points. The set of detection points can include a plurality of detection points. The detection points can, for example, be visually perceivable (e.g., by a client/customer) on an apparatus.
- 30 The authentication method can further include capturing a plurality of images of an identification card (e.g., belonging to the client/customer) using the apparatus. The plurality of images being captured in a manner such that they are capable of coinciding (i.e., in terms of position/location) with the plurality of detection points.

Authentication/verification can be considered to be successful if the captured images coincide (i.e., in terms of position/location) with the detection points.

## 5 **Brief Description of the Drawings**

Embodiments of the disclosure are described hereinafter with reference to the following drawings, in which:

Fig. 1 shows an example of a system which can include at least one apparatus  
10 which can display a set of detection points and at least one host device, according to an embodiment of the disclosure;

Fig. 2 shows an example of the apparatus of Fig. 1 in further detail, according to an  
15 embodiment of the disclosure;

Fig. 3 shows an example implementation in association with the set of detection  
points of Fig. 1, according to an embodiment of the disclosure;

Fig. 4 shows that an example of a computer device which can correspond to, or be  
20 associated with, the apparatus of Fig. 1 and/or the host device of Fig. 1, according to an embodiment of the disclosure;

Fig. 5a shows an example of an authentication method in association with the  
25 system of Fig. 1, according to an embodiment of the disclosure;

Fig. 5b shows an example authentication/verification process embodiment in  
association with the authentication method of Fig. 5a, according to an embodiment of  
the disclosure; and

Fig. 6 shows a diagram illustrating an example of modules of an apparatus which  
30 can, for example, correspond to the apparatus of Fig. 2, according to an embodiment of the disclosure.

## Detailed Description

The present specification contemplates a route-based detection strategy for the purpose of one or both of reliable and efficient authentication/verification, as will be discussed in further detail with reference to Fig. 1 to Fig. 6.

5

Embodiments will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

10 Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art.

15 An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

20

Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “scanning”, “calculating”, “determining”, “replacing”, “generating”, “initializing”, “outputting”, or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

25

system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

30 The present specification also discloses one or more apparatuses for performing the operation(s) of one or more methods. Such apparatus(es) may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer suitable for executing the various methods / processes described herein will appear from the description below.

In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the disclosure.

Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM (Global System for Mobile Communications) mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

The foregoing will be discussed in further detail with reference to Fig. 1 to Fig. 6 hereinafter.

Referring to Fig. 1, a system 100 is shown, according to an embodiment of the disclosure. The system 100 can be associated with a route-based detection strategy for the application/purpose of, for example, authentication/verification.

5 For example, the system 100 can, in the context of authentication/verification, be suitable for use for detecting at least one identification (ID) card which can belong to/be associated with at least one client/customer (i.e., also referable to as at least one user). An ID card can carry, or be associated with, information/data associated with a client/customer, and can be used for the purpose of authentication/verification.

10

The system 100 can include one or more apparatuses 102, one or more host devices 104 and a communication network 106.

The apparatus(es) 102 can be coupled to the host device(s) 104. Specifically, the  
15 apparatus(es) 102 can, for example, be coupled to the host device(s) 104 via the communication network 106.

In one embodiment, the apparatus(es) 102 can be coupled to the communication network 106 and the host device(s) 104 can be coupled to the communication  
20 network 106. Coupling can be by manner of one or both of wired coupling and wireless coupling. The apparatus(es) 102 can, in general, be configured to communicate with the host device(s) 104 via the communication network 106.

The apparatus(es) 102 can, for example, correspond to one or more computers (e.g.,  
25 laptops, desktop computers and/or electronic mobile devices having computing capabilities such as Smartphones and electronic tablets).

In general, the apparatus(es) 102 can be configured to capture information/data associated with a client/customer. Based on the captured information/data (i.e.,  
30 associated with a client/customer), the apparatus(es) 102 can be configured to generate and communicate one or more output signals. For example, the apparatus(es) 102 can be configured to capture at least one image associated with an ID card carrying information/data associated with a client/customer. The output

signal(s) can, for example, be associated with the at least one captured image. In this regard, the apparatus(es) can include one or more capturing parts (e.g., an image capturing device such as a camera), in accordance with an embodiment of the disclosure. Additionally, the apparatus(es) 102 can, for example, include one or  
5 more display parts (e.g., a display such as a screen), in accordance with an embodiment of the disclosure.

Moreover, in general, the apparatus(es) 102 can be configured to receive one or more input signals from the host device(s) 104. The input signal(s) can be  
10 associated with a set of detection points. This will be discussed in further detail hereinafter.

The host device(s) 104 can, for example, correspond to one or more computers (e.g., laptops, desktop computers and/or electronic mobile devices having computing  
15 capabilities such as Smartphones and electronic tablets).

In general, the host device(s) 104 can be configured to generate one or more input signals which can be communicated to the apparatus(es) 102. As mentioned earlier, the input signal(s) can be associated with a set of detection points. For example, the  
20 input signals(s) can be processed to generate a graphics user interface (GUI) which can be displayed on the display(s) of the apparatus(es) 102. The set of detection points can include a plurality of detection points.

In accordance with an embodiment of the disclosure, the input signal(s) can be  
25 communicated from the host device(s) 104 to the apparatus(es) 102 for processing in a manner such that a GUI can be visually perceived on the display(s) of the apparatus(es) 102. The GUI can, for example, correspond to a graphic display of a set of detection points on a display of an apparatus 102 and each detection point can be associated with a position/location on the display of the apparatus 102.

30

Generally, the set of detection points can be graphically displayed in a manner so as to be capable of being visually perceived by a client/customer (e.g., via the display(s) of the apparatus(es) 102).

Based on the input signal(s) received, a client/customer carrying an apparatus 102 can be prompted (e.g., in an audible manner and/or in a visually perceivable manner) to capture one or more images of the client's/customer's ID card based on  
5 corresponding one or more detection points. Specifically, for each detection point displayed, an image of the client's/customer's ID card can be captured in response by the client/customer. In this context, a detection point in the set of detection points can be associated with a corresponding captured image (i.e., a captured image of an ID card which has been captured in response to a displayed detection point).

10

As mentioned earlier, each detection point of the set of detection points can be associated with a position/location displayed on the display of an apparatus 102.

For example, the aforementioned prompt can be by manner of a graphical display of  
15 one or more detection points on the display of the apparatus 102 so that the client/customer can, in response, attempt to capture corresponding at least one image of his/her ID card which can substantially coincide, in terms of location/position, with the displayed detection point(s). Specifically, the client/customer carrying an apparatus 102 can be prompted to use the apparatus  
20 102 to capture one or more images of his/her ID card in a manner such that the captured image(s) coincide, in terms of location/position, with the set of detection points as displayed on the display of the apparatus 102. Therefore, it is appreciable that a captured image (of an ID card) can be associated with a corresponding detection point.

25

Based on the captured image(s), the aforementioned output signal(s) can be generated by the apparatus(es) 102. Moreover, the output signal(s) can, for example, be communicated from the apparatus(es) 102 to the host device(s) 104 for processing.

30

Specifically, in accordance with an embodiment of the disclosure, the host device(s) 104 can be configured to receive and process the output signal(s) in a manner so as to determine whether a captured image substantially coincides with a corresponding

detection point in terms of location/position (e.g., as displayed on the display of an apparatus 102). Processing can, for example, be by manner of comparison-based processing of the input signal(s) and the output signal(s), in accordance with an embodiment of the disclosure.

5

In the event it can be determined (e.g., by manner of comparison-based processing) that the captured image(s) can be considered to substantially coincide with the detection point(s) in terms of location/position, the host device(s) 104 can be configured to determine that authentication/verification can be successfully completed. Otherwise, in the event that it is determined (e.g., by manner of comparison-based processing) that at least one captured image does not coincide with a corresponding detection point in terms of location/position, the host device(s) can be configured to determine a failure in authentication/verification (i.e., authentication/verification cannot be successfully completed). This will be discussed in further detail with reference to Fig. 2, according to an embodiment of the disclosure.

The communication network 106 can, for example, correspond to an Internet communication network and/or a dedicated device-to-device type (e.g., near-field communication type, Bluetooth type, direct wiring type and/or Infra-red type) communication network. Communication (i.e., between the apparatus(es) 102 and the host device(s) 104) via the communication network 106 can be by manner of one or both of wired communication and wireless communication.

Earlier mentioned, the present specification contemplates a route-based detection strategy. Route-based detection can be based the aforementioned set of detection points. Moreover, the set of detection points can be generated based on one or both of a predetermined-based manner and a random-based manner, in accordance with an embodiment of the disclosure. Furthermore, the detection points can be displayed in a sequential manner or a simultaneous manner, in accordance with an embodiment of the disclosure.

In one embodiment, regarding the aforementioned predetermined-based manner, the host device(s) 104 can be configured to generate the input signal(s) such that the detection points of the set of detection points are visually perceivable (e.g., by a client/customer) to be positioned on the display (of an apparatus 102) based on one or more predetermined patterns (as determined by the host device(s) 104). Examples of predetermined patterns can include, for example, a straight-lined pattern, a zig-zag based pattern and one or more patterns based on one or more geometric shapes. Generally, for such a predetermined route-based detection, the position/location associated with a detection point can be considered to be unique (i.e., in the set of detection points, no two detection points share the same location/position).

In one embodiment, regarding the aforementioned random-based manner, the host device(s) 104 can be configured to generate the input signal(s) such that the detection points of the set of detection points are visually perceivable (e.g., by a client/customer) to be random (i.e., no fixed pattern(s) perceivable – e.g., a squiggle). Generally, for such random route-based detection, there is a possibility that a detection point can be associated with the same location/position associated with another detection point (i.e., in the set of detection points, there is a possibility that two or more detection points can share the same location/position). This is possible if the detection points are displayed in a sequential manner as will be discussed later, in accordance with an embodiment of the disclosure.

In one embodiment, regarding display of the set of detection points in a simultaneous manner, a customer/client can visually perceive, at the same time, all the detection points of the set of detection points.

In one embodiment, regarding display of the set of detection points in a sequential manner, only a portion of the set of detection points is displayed at any one time. In one example, only one detection point is displayed at a time and a subsequent detection point is only displayed after it is determined that a corresponding captured image (substantially) coincides (i.e., in terms of position/location) with the displayed detection point (i.e., currently displayed detection point). In another example, at

least two detection points can be displayed initially and a subsequent one or more detection points can only be displayed after it is determined that the corresponding captured images (substantially) coincide (i.e., in terms of position/location) with the initially displayed at least two detection points.

5

The apparatus(es) 102 can now be discussed in further detail with reference to Fig. 2, according to an embodiment of the disclosure, hereinafter.

Referring to Fig. 2, an apparatus 102 is shown in further detail in the context of an example embodiment 200, according to an embodiment of the disclosure.

In the example embodiment 200, the apparatus(es) 102 can include one or more capturing devices 202 and one or more processors 204. The capturing device(s) 202 can be coupled to the processor(s) 204. Coupling can be by manner of one or both of wired coupling and wireless coupling. The apparatus(es) 102 can, for example, further include one or more displays 206. The apparatus(es) 102 can, for example, yet further include one or more transceivers 208. Moreover, the apparatus(es) 102 can, for example, yet further include one or more memory devices (not shown).

20

Each of the capturing device(s) 202, the display(s) 206, the transceiver(s) 208, the memory device(s) or any combination thereof, can be coupled to the processor(s) 204. Coupling can be by manner of one or both of wired coupling and wireless coupling.

25

The capturing device(s) 202 can be configured to capture information/data associated with a client/customer. In one example, a capturing device 202 can correspond to an image capturing device (e.g., a camera) which can be configured to capture at least one image associated with an ID card associated with a client/customer.

30

Based on the captured information/data (i.e., associated with a client/customer), the capturing device(s) 202 can be configured to generate and communicate one or

more captured signals which can be associated with one or more captured images of the ID card. The captured signal(s) can be communicated from the capturing device(s) 202 to the processor(s) 204. The processor(s) 204 can be configured to receive and process the captured signal(s) to generate one or more output signals.

5 The output signal(s) can, for example, be communicated from apparatus(es) 102 to the host device(s) 104 via the transceiver(s) 208, in accordance with an embodiment of the disclosure. Moreover, the input signal(s) from the host device(s) 104 can be received by the apparatus(es) 102 via the transceiver(s) 208, in accordance with an embodiment of the disclosure.

10

The processor(s) 204 can be configured to perform one or more processing tasks in respect of one or both of the captured signal(s) and the input signal(s) to generate the output signal(s), in accordance with an embodiment of the disclosure.

15 In one embodiment, the processor(s) 204 can be configured to perform detection-based processing (e.g., linear regression-based processing) in connection with the captured signal(s). For example, in regard to linear regression-based processing, location of each corner (e.g., four corners) of the ID card can be predicted, and based on the predicted location of each corner of the ID card, the center of the ID  
20 card can be derived/determined.

In one embodiment, the processor(s) 204 can be configured to perform image-based processing in connection with the input signal(s) in a manner so as to graphically render (e.g., in the form of a GUI) the set of detection points do that the detection  
25 point(s) can be visually perceivable via the display(s) 206.

In one embodiment, the memory device(s) can carry a set of instructions that when executed (e.g., by the processor(s) 204):

- causes the at least one display 206 to display a set of detection points, each  
30 detection point in the set of detection points being associable with a position on the display 206;

- causes the at least one capturing device 202 to capture data associated with an Identification (ID) Card which is associated with a customer, captured data being associated with at least one image of the ID card; and

- 5
- causes the at least one processor 204 to process the captured data to determine at least one of location of each corner of the ID card and center of the ID card,

To put the forgoing in general perspective, the present specification contemplates, in accordance with an embodiment, an apparatus 102 (e.g., a Smartphone) which can be associated with an authentication/verification process. The authentication/verification process can be associated with an authentication method which will be discussed later in further detail with reference to Fig. 5, in accordance with an embodiment of the disclosure.

15

The apparatus 102 can include a capturing device 202 (e.g., a camera), a processor 204 (e.g., a microprocessor) and a display 206 (e.g., a screen), in accordance with an embodiment of the disclosure.

20 The capturing device 202 and the display 206 can, in one embodiment, be coupled to the processor 204.

The capturing device 202 can capture data associated with an Identification (ID) Card. The ID card can be associated with a customer. Moreover, captured data can be associated with at least one image of the ID card (i.e., at least one captured image of an ID card).

The processor 204 can process the captured data in a manner so as to determine at one or both of location of each corner of the ID card and center of the ID card (i.e., location of each corner of the ID card and/or center of the ID card).

30

The display 206 can display a set of detection points. Each detection point in the set of detection points can be associated with a position/location on the display 206.

Moreover, the apparatus 102 can be controlled (e.g., by the customer, by manner of positioning the apparatus 102 with respect to the ID card and/or positioning the ID card with respect to the apparatus 102) so that the capturing device 202 can capture  
5 an image of the ID card in a manner so as to coincide (e.g., in terms of location/position) with a corresponding detection point. Successful authentication can, for example, be determined after all taken images of the ID card (i.e., captured images of the ID card) have been determined to coincide with the corresponding detection points.

10

In one embodiment, the set of detection points can include at least one initial detection point and at least one subsequent detection point. The set of detection points can be displayed on the display 206 in a sequential manner such that the initial detection point is displayed followed by at least one subsequent detection point.

15

In one example, at least one subsequent detection point is displayed only after it has been determined (e.g., by the aforementioned host device 104) that an image of the ID card taken in response to the displayed initial detection point coincides with the initial detection point. Moreover, the authentication process can, for example, be aborted due to failure to display at least one subsequent detection point after a  
20 predetermined time period with respect to the time when the initial detection point was displayed.

20

In another embodiment, the set of detection points can include a plurality of detection points. The detection points can be displayed on the display 206 in a simultaneous  
25 manner such that the detection points are visually perceivable at the same time (i.e., simultaneously). The authentication process can, for example, be aborted due to failure of a taken image (i.e., a captured image) and a corresponding detection coinciding after a predetermined time period.

25

30

The present specification contemplates, in accordance with another embodiment, an apparatus 102 (e.g., a Smartphone) which can be associated with an authentication/verification process. The authentication/verification process can be

associated with an authentication method which will be discussed later in further detail with reference to Fig. 5, in accordance with an embodiment of the disclosure.

5 The apparatus 102 can include at least one display 206 and at least one capturing device 202. The apparatus 102 can further include at least one processor 204 coupled to one or both of the at least one display 206 and the at least one capturing device 202

10 The apparatus 102 can further include at least one memory device (not shown) coupled to the processor. The memory device can carry a set of instructions that when executed (e.g., by the processor(s) 204):

- 15 • causes the at least one display 206 to display a set of detection points, each detection point in the set of detection points being associable with a position on the display 206;
- causes the at least one capturing device 202 to capture data associated with an Identification (ID) Card which is associated with a customer, captured data being associated with at least one image of the ID card; and
- 20 • causes the at least one processor 204 to process the captured data to determine at least one of location of each corner of the ID card and center of the ID card,

25 An image of the ID card can be captured so as to coincide with a corresponding detection point.

The set of detection points will be discussed in the context of an example implementation, in accordance with an embodiment of the disclosure hereinafter.

30 Referring to Fig. 3, an example implementation 300 in association of with a set of detection points 302 is shown, in accordance with an embodiment of the disclosure.

As shown, the set of detection points 302 can include a plurality of detection points (e.g., a first detection point 302a, a second detection point 302b, a third detection point 302c and a fourth detection point 302d).

- 5 In one embodiment, with regard to sequential display-based manner of the set of detection points, the first detection point 302a can correspond to the aforementioned initial detection point and the second to fourth detection points 302b/302c/302d can correspond to the aforementioned at least one subsequent detection point.
- 10 In one embodiment, with regard to simultaneous display-based manner of the set of detection points, the first to fourth detection points 302a/302b/302c/302d can be visually perceivable on the display 206 at the same time (i.e., simultaneously). Moreover, the first to fourth detection points 302a/302b/302c/302d can, for example, be visually perceivable to be displayed based on a predetermined pattern (e.g., a
- 15 zig-zag based pattern).

Moreover, the present specification contemplates that the set of detection points can include less or more detection points than the first to fourth detection points 302a/302b/302c/302d as shown in Fig. 3.

20

- In view of the foregoing manner of authentication/verification, it is appreciable that a client/customer would be required to actually use an ID card and capture images of the ID card based on the aforementioned set of detection points. It is contemplated that an unauthorized party/individual attempting to use a high resolution screen shot
- 25 of an ID card would at least have significant difficulties in passing off any such high resolution screen shot of the ID card as authentic since the screen shot would not be considered to be captured in the earlier discussed manner in relation to the set of detection points. In this manner, reliability in authentication/verification could possibly be improved as circumvention can be impeded.

30

Moreover, it is contemplated that by manner of capturing images of the ID card based on the aforementioned set of detection points, complex training and/or reliance on large data samples etc. would not be required. Therefore verification

techniques which would require large amount of data and/or large-scale training samples (e.g., Moiré pattern-based analysis) would not be necessary. In this manner, efficiency in authentication/verification can potentially be improved.

- 5 The present specification contemplates that in one example, an apparatus 102 and/or a host device 104 can correspond to/be associated with a computing device. This will be discussed in the context of an example computing device with reference to Fig. 4 hereinafter.
- 10 Fig. 4 shows, according to an embodiment of the disclosure, an example computing device 400, hereinafter interchangeably referred to as a computer system 400. The following description of the computing device 400 is provided by way of example only and is not intended to be limiting.
- 15 As shown in Fig 4, the example computing device 400 includes a processor 404 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 400 may also include a multi-processor system. The processor 404 is connected to a communication infrastructure 406 for communication with other components of the computing device 400. The communication infrastructure 406 may include, for example, a communications bus, cross-bar, or network.
- 20

The computing device 400 further includes a main memory 408, such as a random access memory (RAM), and a secondary memory 410. The secondary memory 410 may include, for example, a hard disk drive 412 and/or a removable storage drive 414, which may include a floppy disk drive, a magnetic tape drive, an optical disk drive, or the like. The removable storage drive 414 reads from and/or writes to a removable storage unit 418 in a well-known manner. The removable storage unit 418 may include a floppy disk, magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 414. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 418 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

25

30

In an alternative implementation, the secondary memory 410 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 400. Such means can include, for example, a removable storage unit 422 and an interface 420. Examples of a removable storage unit 422 and interface 420 include a program cartridge and cartridge interface (such as that found in video game console devices), a removable memory chip such as an EPROM (erasable programmable read-only memory) or PROM (programmable read-only memory) and associated socket, and other removable storage units 422 and interfaces 420 which allow software and data to be transferred from the removable storage unit 422 to the computer system 400.

The computing device 400 also includes at least one communication interface 424. The communication interface 424 allows software and data to be transferred between computing device 400 and external devices via a communication path 426. In various embodiments of the disclosure, the communication interface 424 permits data to be transferred between the computing device 400 and a data communication network, such as a public data or private data communication network. The communication interface 424 may be used to exchange data between different computing devices 400 which such computing devices 400 form part an interconnected computer network. Examples of a communication interface 424 can include a modem, a network interface (such as an Ethernet card), a communication port, an antenna with associated circuitry and the like. The communication interface 424 may be wired or may be wireless. Software and data transferred via the communication interface 424 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 424. These signals are provided to the communication interface via the communication path 426.

As shown in Fig 4, the computing device 400 further includes a display interface 402 which performs operations for rendering images to an associated display 430 and an audio interface 432 for performing operations for playing audio content via associated speaker(s) 434.

As used herein, the term "computer program product" may refer, in part, to removable storage unit 418, removable storage unit 422, a hard disk installed in hard disk drive 412, or a carrier wave carrying software over communication path 426  
5 (wireless link or cable) to communication interface 424.

Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 400 for execution and/or processing. Examples of such storage media include floppy  
10 disks, magnetic tape, CD-ROM (compact disc read-only memory), DVD (Digital Versatile Disc/Digital Video Disc), Blu-ray™ Disc, a hard disk drive, a ROM (Read-only memory) or integrated circuit, USB (Universal Serial Bus) memory, a magneto-optical disk, or a computer readable card such as a PCMCIA (Personal Computer Memory Card International Association) card and the like, whether or not such  
15 devices are internal or external of the computing device 400. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 400 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or  
20 Intranets including e-mail transmissions and information recorded on Websites and the like.

The computer programs (also called computer program code(s)/algorithm(s)) are stored in main memory 408 and/or secondary memory 410. Computer programs can  
25 also be received via the communication interface 424. Such computer programs, when executed, enable the computing device 400 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 404 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers  
30 of the computer system 400.

Software may be stored in a computer program product and loaded into the computing device 400 using the removable storage drive 414, the hard disk drive

412, or the interface 420. Alternatively, the computer program product may be downloaded to the computer system 400 over the communications path 426. The software, when executed by the processor 404, causes the computing device 400 to perform functions of embodiments described herein.

5

It is to be understood that the embodiment of Fig. 4 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 400 may be omitted. Also, in some embodiments, one or more features of the computing device 400 may be combined together. Additionally, in some  
10 embodiments, one or more features of the computing device 400 may be split into one or more component parts.

It will be appreciated that the elements illustrated in Fig. 4 function to provide means for performing the various functions and operations of the servers as described in the  
15 above embodiments.

In an implementation, a server may be generally described as a physical device comprising at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are  
20 configured to, with the at least one processor, cause the physical device to perform the requisite operations.

Referring to Fig. 5a, an authentication method 500 in association with the system 100 is shown, according to an embodiment of the disclosure. The authentication  
25 method 500 can be useful for authentication/verification (e.g., authentication/verification in association with one or more clients/customers via the use of ID card(s) belonging to the client(s)/customer(s)).

The authentication method 500 can include any one of an input (or “inputting”) step  
30 502, an output (or “outputting”) step 504 and a processing (or “generating”) step 506, or any combination thereof.

In regard to the input step 502, one or more input signals can be communicated to the apparatus 102. The input signal(s) can be associated with a set of detection points which can include a plurality of detection points.

- 5 In regard to the output step 504, one or more output signals can be generated by the apparatus 102. The output signal(s) can, for example, be associated with one or more captured images of an ID card belonging to a client/customer.

10 In regard to the processing step 506, the output signal(s) can be processed in a manner so as to determine whether the capture image(s) coincide with the plurality of detection points. In one embodiment, the output signal(s) can be processed by, for example, the host device 104.

15 Generally, the present specification contemplates an authentication method 500 which can include providing a set of detection points. The set of detection points can include a plurality of detection points (302a/302b/302c/302d). The detection points (302a/302b/302c/302d) can, for example, be visually perceivable (e.g., by a client/customer) on an apparatus 102 (e.g., via a display of the apparatus 102).

20 The authentication method 500 can further include capturing a plurality of images of an identification card (e.g., belonging to the client/customer) using the apparatus 102. The plurality of images being captured in a manner such that they are capable of coinciding (i.e., in terms of position/location) with the plurality of detection points (302a/302b/302c/302d).

25 Authentication/verification can be considered to be successful if the captured images coincide (i.e., in terms of position/location) with the detection points.

30 The present specification contemplates that, in one embodiment, the apparatus 102 can be moveably controlled (e.g., by the client/customer) when capturing the plurality of images. The apparatus 102 can be moveably controlled in a manner such that the captured plurality of images can coincide with the set of detection points, in terms of location/position the plurality of detection points are displayed on the apparatus 102.

Referring to Fig. 5b, a flow diagram of an example authentication/verification process embodiment 550 associated with the authentication method 500 is shown, in accordance with an embodiment of the disclosure.

5

The example authentication/verification process embodiment 550 can, for example, include a first step 550a, a second step 550b, a third step 550c, a fourth step 550d, a fifth step 550e and a sixth step 550f, or any combination thereof.

10 At the first step 550a (i.e., "Start"), a user (e.g., a customer/client) can hold the ID card using one hand and using the apparatus 102, held by another hand, to capture an image of the ID card.

At the second step 550b (i.e., "Detect ID of start point"), the user can be prompted to  
15 position the ID card so as to coincide with the first detection point 302a (as displayed on the display screen of the apparatus 102). An ID card detection method (e.g., a linear regression method to predict the corners of the ID card and computing the center of the ID card based on predicted location of the corners) can be used to determine (e.g., predict) the ID card's localization. If it can be determined (i.e., "ID  
20 card exist?") that the ID card's localization matches the first detection point 302a, the user can be prompted to position the ID card so as to coincide with the second detection point 302b (i.e., "Y" indication to proceed to the third step 550c). Otherwise (i.e., the ID card's localization does not match the first detection point 302a), authentication/verification can be deemed to be unsuccessful (i.e., "N"  
25 indication) and, for example, terminated/aborted (e.g., by manner of returning to the first step 550a/impeding progress to the third step 550c/remaining in the second step 550b where the user can, for example, be continually prompted to reposition the ID card with respect to the first detection point 302a). In one embodiment, if, within a certain period (e.g., a time period of 15 seconds or 30 seconds), the ID card cannot  
30 be detected, authentication/verification can be terminated/aborted (e.g., by manner of returning to the first step 550a/impeding progress to the third step 550c/remaining in the second step 550b).

At the third step 550c (i.e., "Detect ID of B point"), the user can be prompted to position the ID card so as to coincide with the second detection point 302b (as displayed on the display screen of the apparatus 102). The third step 550c can be analogous to the second step 550b. In this regard, relevant portions of the earlier discussion in relation to the second step 550b analogously apply to the third step 550c. If it can be determined (i.e., "ID card exist?") that the ID card's localization matches the second detection point 302b, the user can be prompted to position the ID card so as to coincide with the third detection point 302c (i.e., "Y" indication to proceed to the fourth step 550d). Otherwise (i.e., the ID card's localization does not match the second detection point 302b), authentication/verification can be deemed to be unsuccessful (i.e., "N" indication) and, for example, terminated/aborted (e.g., by manner of returning to the first step 550a or the second step 550b/impeding progress to the fourth step 550d/remaining in the third step 550c where the user can, for example, be continually prompted to reposition the ID card with respect to the second detection point 302b). In one embodiment, if, within a certain period (e.g., a time period of 15 seconds or 30 seconds), the ID card cannot be detected, authentication/verification can be terminated/aborted (e.g., by manner of returning to the first step 550a or the second step 550b/impeding progress to the fourth step 550d/remaining in the step 550c).

20

At the fourth step 550d (i.e., "Detect ID of C point"), the user can be prompted to position the ID card so as to coincide with the third detection point 302c (as displayed on the display screen of the apparatus 102). The fourth step 550d can be analogous to the second step 550b. In this regard, relevant portions of the earlier discussion in relation to the second step 550b analogously apply to the fourth step 550d. If it can be determined (i.e., "ID card exist?") that the ID card's localization matches the third detection point 302c, the user can be prompted to position the ID card so as to coincide with the fourth detection point 302d (i.e., "Y" indication to proceed to the fifth step 550e). Otherwise (i.e., the ID card's localization does not match the third detection point 302c), authentication/verification can be deemed to be unsuccessful (i.e., "N" indication) and, for example, terminated/aborted (e.g., by manner of returning to the first step 550a or the third step 550c/impeding progress to the fifth step 550e/remaining in the fourth step 550d where the user can, for example,

be continually prompted to reposition the ID card with respect to the third detection point 302c). In one embodiment, if, within a certain period (e.g., a time period of 15 seconds or 30 seconds), the ID card cannot be detected, authentication/verification can be terminated/aborted (e.g., by manner of returning to the first step 550a or the  
5 third step 550c/impeding progress to the fifth step 550e/remaining in the fourth step 550d).

At the fifth step 550e (i.e., "Detect ID of end point"), the user can be prompted to position the ID card so as to coincide with the fourth detection point 302d (as  
10 displayed on the display screen of the apparatus 102). The fifth step 550e can be analogous to the second step 550b. In this regard, relevant portions of the earlier discussion in relation to the second step 550b analogously apply to the fifth step 550e. If it can be determined (i.e., "ID card exist?") that the ID card's localization matches the fourth detection point 302d, verification/authentication can be  
15 considered to be successful (i.e., "Y" indication to proceed to the sixth step 550f). Otherwise (i.e., the ID card's localization does not match the fourth detection point 302d), authentication/verification can be deemed to be unsuccessful (i.e., "N" indication) and, for example, terminated/aborted (e.g., by manner of returning to the first step 550a or the fourth step 550d/impeding progress to the sixth step  
20 550f/remaining in the fifth step 550e where the user can, for example, be continually prompted to reposition the ID card with respect to the fourth detection point 302d). In one embodiment, if, within a certain period (e.g., a time period of 15 seconds or 30 seconds), the ID card cannot be detected, authentication/verification can be terminated/aborted (e.g., by manner of returning to the first step 550a or the fourth  
25 step 550d/impeding progress to the sixth step 550f/remaining in the fifth step 550e).

At the sixth step 550f (i.e., "Finish"), verification/authentication can be deemed to be successful and completed.

30 It is appreciable that based on the above discussed steps (first to sixth steps 550a/550b/550c/550d/550e, or any combination thereof), attempts to circumvent authentication/verification by manner of, for example, producing a high quality screen-shot of an ID card can be impeded. In this regard, integrity of

verification/authentication can be preserved. Appreciably, a robust verification/authentication process/method per the earlier discussed authentication method 500 (and example authentication/verification process embodiment 550 in association therewith), can be facilitated.

5

Referring to Fig. 6, an example of modules of an apparatus 600 is shown according to an embodiment of the disclosure. The apparatus 600 can be an example of an embodiment of the aforementioned apparatus 102.

10 As shown, the apparatus 600 can include a first module 602 and a second module 604. The first module 602 can be associated with the aforementioned capturing device(s) 202. The second module 604 can be associated with the aforementioned processor(s) 204.

15 Specifically, the apparatus 600 can include a first module 602 that obtains/captures data/information associated with a client/customer to generate and communicate one or more captured signals.

The apparatus 600 can further include a second module 602 that processes the  
20 captured signal(s) and/or the aforementioned received input signal(s) to generate one or more output signal(s).

Fig. 6 can, for example, be interpreted as illustrating an internal functional module and/or a structure of an apparatus (i.e., the aforementioned apparatus 102) which  
25 can be associated with a route-based detection strategy for the purpose of one or both of reliable and efficient authentication/verification, according to an embodiment of the disclosure.

It should be further appreciated by the person skilled in the art that variations and  
30 combinations of features described above, not being alternatives or substitutes, may be combined to form yet further embodiments.

In one example, although the foregoing discussion has generally been in the context of one or more ID cards, the present specification contemplates that other forms of identification (for the purpose of verification/authentication) can be useful. An example is facial based recognition (i.e., Face ID).

5

In another example, it is earlier discussed that the host device(s) 104 can be configured to receive and process the output signal(s) in a manner so as to determine whether a captured image substantially coincides with a corresponding detection point in terms of location/position. The present specification contemplates that, in accordance with an embodiment of the disclosure, determination (e.g., by manner of comparison-based processing) of whether a captured image substantially coincides with a corresponding detection point can be done/performed at the apparatus(es) 102 (in which case, communication of the output signal(s) to the host device(s) 104 can be optional). Therefore, it is appreciable that one or both of the apparatus(es) 102 and the host device(s) 104 can be configured to determine (e.g., by manner of comparison-based processing) whether a captured image substantially coincides with a corresponding detection point in terms of location/position, in accordance with an embodiment of the disclosure.

20 In yet another example, instead of movably controlling the apparatus(es) 102 to capture one or more images of an ID card(s), the ID card(s) can be movably controlled while the apparatus(es) 102 remain(s) stationary.

In yet a further example, the apparatus(es) 102 and the ID card(s) can be moveably controlled relative to each other (e.g., the apparatus(es) 102 and the ID card(s) can be simultaneously moved relative to each other).

30 In the foregoing manner, various embodiments of the disclosure are described for addressing at least one of the foregoing disadvantages. Such embodiments are intended to be encompassed by the following claims, and are not to be limited to specific forms or arrangements of parts so described and it will be apparent to one skilled in the art in view of this disclosure that numerous changes and/or modification can be made, which are also intended to be encompassed by the following claims.

## Claim(s)

1. An apparatus comprising:
- at least one display;
- 5 at least one image capturing device;
- at least one processor coupled to the at least one display and the at least one image capturing device ; and
- at least one memory device, coupled to the at least one processor, storing a set of instructions for execution by the at least one processor, the
- 10 set of instructions instruct the at least one processor to:
- cause the at least one display to display first at least one detection point corresponding to first at least one position on the at least one display;
- cause the at least one image capturing device to capture a first
- 15 image of an Identification (ID) card associated with a customer; and
- process the first image to determine at least one of a location of each corner of the ID card or a location of a center of the ID card;
- determine, based on the at least one of the location of each corner of the ID card or the location of the center of the ID card, that
- 20 the first image of the ID card matches the first at least one detection point; and
- cause the at least one display to prompt the customer to reposition the at least one image capturing device so that a second image of the ID card is captured to coincide with second at least one
- 25 detection point corresponding to second at least one position on the at least one display,
- wherein the first at least one detection point and the second at least one detection point are displayed in a simultaneous manner and are visually distinguishable.
- 30

2. The apparatus as in claim 1, wherein the apparatus is associable with an authentication process and successful authentication is determinable after the first and second images have been determined to coincide with the corresponding detection points.

5

3. An authentication method comprising:

providing first at least one detection point corresponding to first at least one position on at least one display;

10 capturing a first image of an identification (ID) card associated with a customer;

processing the first image to determine at least one of a location of each corner of the ID card or a location of a center of the ID card;

15 determining, based on the at least one of the location of each corner of the ID card or the location of a center of the ID card, that the first image of the ID card matches the first at least one detection point; and

causing the at least one display to prompt the customer to reposition at least one image capturing device used to capture the first image so that a second image of the ID card is captured to coincide with second at least one position on the at least one display,

20 wherein the first at least one detection point and the second at least one detection point are displayed in a simultaneous manner and are visually distinguishable.

25

30