

data into which the input data are compared. The subset of unique identifier data is randomly selected from a set of unique identifier data generated from any one or more color identifier data in a standardized color matching system such as the Pantone Matching System which provides unique color values
5 whereby no same digital key can be generated for the object of authentication.

The provision of generating the digital key based on the relative distance of the randomly selected and overlaid unique identifier data originating from color identifier data in the standardized color matching system, such as the well-known Pantone Matching System, guarantees the
10 uniqueness of the digital key for each object of authentication. In other words, this arrangement guarantees that no same digital key can be generated for a single object of authentication. Security risks which are associated with identical pass codes in authentication systems and high level of authentication are thereby substantially reduced, if not totally eliminated. Further, security
15 level of authentication is significantly increased with this provision of digital key generation used in conjunction with other authentication modalities in one or more technical frameworks for multimodal authentication determination.

According to one aspect, there is provided a computer-implemented method of controlling access to an identity-based access-controlled resource
20 using multimodal authenticity determination, the multimodal authenticity determination being directed to an object of authentication at an access point located in the access-controlled resource. The method includes: receiving a first input data including information on a first modality associated with the object of authentication; deriving a first authentication data from the
25 information on the first modality based on at least one first authentication parameter, the at least one first authentication parameter being based on the first modality; determining at least one first authenticity score for the object of

authentication by comparing the first authentication data with a first reference authentication data associated with the object of authentication and stored in an electronic database; receiving a second input data including information on a second modality associated with the object of authentication based on
5 acceptability of the determined at least one first authenticity score; deriving a second authentication data from the information on the second modality based on at least one second authentication parameter, the at least one second authentication parameter being based on the second modality; determining at least one second authenticity score for the object of authentication by
10 comparing the second authentication data with a second reference authentication data associated with the object of authentication and stored in the electronic database; receiving a third authentication data uniquely identifying the any of the first and second input data based on acceptability of the determined at least one second authenticity score; determining at least one
15 third authenticity score for the object of authentication by comparing the third authentication data with a third reference authentication data associated with the object of authentication and stored in the electronic database; and causing an access control unit at the access point to grant access to the access-controlled resource based on acceptability of the determined at least one third
20 authenticity score, wherein the third reference authentication data includes at least one digital key generated based at least in part on a determined distance of at least two unique identifier data in relation to one another, the at least two unique identifier data being included in a subset of unique identifier data overlaid to any of a reference first input data into which the first input data is
25 compared and a reference second input data into which the second input data is compared, the subset of unique identifier data being randomly selected from a set of unique identifier data, the set of unique identifier data being generated from any one or more color identifier data in a standardized color matching system.

According to further aspects, the computer-implemented method according to the aforesaid aspect of the present specification may be implemented using a computer-based system, a terminal, an electronic device or a computer program product, or any combination thereof. The computer-based system, terminal or electronic device may include a plurality of authentication modules and an access control module for controlling access to an identity-based access-controlled resource using multimodal authenticity determination, the multimodal authenticity determination being directed to an object of authentication at an access point located in the access-controlled resource.

For a better understanding of the invention and to show how the same may be performed, preferred implementations and/or embodiments thereof will now be described, by way of non-limiting examples only, with reference to the accompanying drawings.

Brief Description of the Several Views of the Drawings

Figure 1 is a flow diagram illustrating a method of controlling access to an identity-based access-controlled resource consistent with one or more embodiments of the invention.