

intended to identify key features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

In at least one aspect of the present disclosure, a handwriting verification method executed in a computer system comprises obtaining a handwriting test sample containing a plurality of available parameters, wherein the plurality of available parameters comprises geometric parameters and one or more non-geometric parameters; extracting the geometric parameters from the plurality of available parameters; based on the geometric parameters, deriving geometric features comprising an x-position value and a y-position value for each of a plurality of evenly distributed feature points in the handwriting test sample; performing first feature matching between geometric features of the handwriting test sample and geometric features of a reference sample; determining a handwriting verification result based at least in part on the feature matching; and outputting the handwriting verification result. The geometric features may further comprise values derived from the geometric parameters, such as direction and curvature values. The determining of the handwriting verification result can be further based on a count of unlinked feature points.

The first feature matching can include finding mappings between one or more of the evenly distributed feature points in the test sample and one or more evenly distributed feature points in the reference sample. The first feature matching can include a simulated annealing process. The simulated annealing process can include selecting a feature point in the reference sample; generating a pseudo-random value; comparing the pseudo-random value with a constant; and based on the comparing, determining whether to remove a link from a selected point in the reference sample or define a new link between the selected feature point in the reference sample and a selected feature point in the test sample. The determining step can be biased towards defining a new link over removing an existing link based on the value of the constant. If a new link is defined, any previously existing links that are crossed by the new link can be removed.

Second feature matching also can be performed, which may include evaluation of a non-geometric parameter (e.g., a time-related parameter, such as speed or acceleration). The handwriting verification result can be further based on the second feature matching.

In another aspect, a handwriting verification method executed in a computer system comprises performing feature matching between geometric features of a

handwriting test sample and geometric features of a reference sample, wherein the feature matching comprises defining one or more links

between one or more evenly distributed feature points in the test sample and one or more evenly distributed feature points in the reference sample; obtaining a count of consecutive unlinked feature points in the test sample; and outputting a handwriting verification result, wherein the handwriting verification result is based at least in part on the feature matching and the count of consecutive unlinked feature points in the test sample.

In another aspect, a user authentication method executed in a computer system comprises receiving test signature data and a user device identifier (ID) from a user device; searching for a name or user ID associated with the test signature data; obtaining the name or user ID; searching for a reference device ID associated with the name or user ID; comparing the reference device ID with the user device ID; and providing authentication information (e.g., an authentication result) to the user device based on the comparing. The device IDs may be, for example, pen or stylus IDs associated with a pen or stylus.

In another aspect, a user authentication method executed in a computer system comprises receiving test signature data (e.g., encrypted test signature data), a device identifier, and a service identifier from a user device, wherein the service identifier relates to a service executing on the user device; comparing the test signature data with reference signature data to determine whether the test signature data is consistent with the reference signature data; based on a result of the comparing, obtaining authentication information (e.g., a user ID and a password) associated with the service executing on the user device; and providing the authentication information to the user device. If the test signature data is consistent with the reference signature data, the test signature data may be added to the reference signature data (e.g., as supplemental information for future authentications).

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1A is a high-level diagram of an illustrative cloud computing arrangement configured to verify authenticity of sample handwriting data;

FIGURE 1B is a functional block diagram of an illustrative handwriting data processing section;

FIGURE 2A is an illustration of a handwritten signature comprising a plurality of pen events;

FIGURE 2B is a diagram of rotation, altitude, and azimuth parameters that can be detected for a pen device;