

visual password is robust if it allows a user to be authenticated by entering an input pattern that approximates the secret pattern within specific parameters. For security purposes, it is better to store the visual password in a form from which it is difficult to recover the secret pattern, yet still possible to verify that the correct visual password was entered.

[0064] The graphical interface **112** (**FIG. 1**) receives a secret pattern from a user (**STEP 210**). The secret pattern is a sequence of discrete graphical inputs. In some embodiments, a discrete graphical input is the selection of a region on the graphical interface **112**.

[0065] For example, as illustrated in the example of **FIG. 3**, one embodiment displays boundaries of a plurality of regions on the graphical interface **112**. As further illustrated in **FIG. 3**, one embodiment displays a unique icon within the boundary of each region on the graphical interface **112**. In one embodiment, an icon associated with a region is shown on the bottom of the graphical interface **112** after it is selected. In the embodiment illustrated by **FIG. 3**, three icons **310**, **320**, **330** associated with three different regions are shown in order on the bottom of the graphical interface **112** after having been selected.

[0066] An alternative approach to the selection of regions in accordance with another embodiment of the invention is illustrated in **FIG. 4**. In this embodiment, the graphical interface **112** does not indicate the boundaries of the regions that may be selected by the user. In one such embodiment, selected regions are highlighted after selection. In the embodiment illustrated by **FIG. 4**, three regions **401** are numbered in the order that they were selected and highlighted.

[0067] A discrete graphical input in another embodiment is the selection of a point. As illustrated in **FIG. 5**, one embodiment displays an image on the graphical interface **112** while the user is in the process of selecting a point **510**. In a related embodiment, the graphical interface **112** displays a new image after the user selects a point. The user can thereby associate a particular point selection with a corresponding image, and use the image as a memory aid. Such an embodiment may have a sequence of images that are first used during the enrollment process to prompt the user to select a sequence of points, which will comprise the secret pattern, and later used to prompt the user to enter the same sequence of points to authenticate himself.

[0068] In the context of this discussion, a point is not limited to its strict geometric definition. Instead, a point refers to a relatively small contiguous portion of a graphical interface. A point may be a single pixel of a graphical interface if the input capability allows that level of discrimination. Alternately, a point may be a group of pixels (for example, **10**, **20**, **100**, or more pixels) on the graphical interface, the size of which is approximately consistent with the discrimination level of the input capability associated with the graphical interface, with the user, or with both. A region refers to a larger portion of a graphical interface, and is thereby distinguishable from a point.

[0069] As illustrated in **FIG. 6**, one embodiment presents the user with a memory cue **604** when a point **610** on the graphical interface **112** is highlighted. **FIG. 6** illustrates an embodiment in which an icon **604** is associated with a point

**610** that may be selected on the graphical interface **112**. In such an embodiment, highlighting different points on the graphical display **112** causes different icons to be presented on the graphical display **112**. The user can thereby associate a particular point selection with a pop-up icon, and use the icon during the authentication process to remember the point. In alternative embodiments, the memory cue is auditory. In other embodiments, memory cues include visual and auditory cues.

[0070] As illustrated in **FIG. 7**, one embodiment presents the user with a choice of points **710**, **720** on the graphical interface. A user has the option of selecting point **710** or point **720** in **FIG. 7**. Related embodiments will present more than two choices to the user. Some embodiments display all available points at once. Other embodiments alternate the available points on display. Such embodiments prevent a user from limiting their selection to the most salient features of an image. When incorporated into embodiments that do not display an image, such embodiments prevent a user from limiting their selection to the most easily remembered points on the graphical interface **112**.

[0071] Returning again to **FIG. 2**, the converter **114** (**FIG. 1**) converts each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values (**STEP 220**). The sequence of discrete graphical inputs, which forms the secret pattern, is thereby converted to a sequence of values. A converter, in one embodiment, simply converts a selected portion of the graphical interface into a value that designates that portion. Existing graphical interfaces **112** often incorporate such a converter **114**. In an alternative embodiment, a converter that is distinct from the graphical interface **112** converts a discrete graphical choice into an associated value. In one such embodiment, the value represents a truncated designation of the discrete graphical choice. In another such embodiment, the value represents a compressed designation of the discrete graphical choice. In another such embodiment, the value represents a padded designation of the discrete graphical choice. In another embodiment, each point or region on the graphical interface is associated with an arbitrary string. In one such embodiment the arbitrary string is binary. Such an embodiment may convert a discrete graphical choice into a value by looking up a value associated with the discrete graphical choice on a table.

[0072] The codeword generator **116** (**FIG. 1**) generates a codeword for each value in the sequence of values to produce a sequence of codewords (**STEP 230**). Since more than one value will generate the same codeword, the generation of a codeword is intended to create an approximation parameter for each value such that all values that fall within the approximation parameter of a specific value will be deemed to match that specific value. Embodiments of the invention may use a portion of an error-correcting code to create the approximation parameter.

[0073] Referring to **FIG. 8**, an error-correcting code is used to enable transmission of a message intact over a noisy communication channel. A message  $m$  to be transmitted is chosen from message space **10**. The set of messages  $M$  in message space **10** may be represented mathematically as  $M = \{0, 1\}^k$  where each message  $m$  in the set of messages  $M$  is a binary  $k$ -bit string. There are  $2^k$  messages in the set of messages  $M$  because each bit in the  $k$ -bit string can have one of two values.