

embodiment, the method also includes displaying an image on the graphical interface after receiving the selected point on the graphical interface. In one such embodiment, each discrete graphical choice in the sequence of discrete graphical choices is associated with one of a plurality of images. In one embodiment, the method also includes associating an icon from a plurality of icons with a point on the graphical interface by displaying the icon when the point is highlighted.

[0027] In one embodiment, the graphical interface displays a fractal image. In a related embodiment, the method further includes adjusting the perspective of the fractal image on the graphical interface after receiving an input value in the sequence of input values. Adjusting the perspective includes zooming in and/or zooming out on the fractal image in some embodiments.

[0028] In one embodiment, a discrete graphical choice in the sequence of discrete graphical choices includes a selected icon from a plurality of icons on the graphical interface. In one embodiment, the icon on the graphical interface represents a face. In one embodiment, access to a resource is granted in response to the step of authenticating the user. In one embodiment, access is granted to one or more of a hardware device, a computer system, a portable computer, a software application, a database, and a physical location.

[0029] In general, in another aspect, the invention relates to an apparatus for establishing a secret to authenticate a user. The apparatus includes a graphical interface capable of receiving graphical input. The graphical interface receives a secret pattern as graphical input. The secret pattern includes a sequence of discrete graphical choices. The apparatus includes a converter in signal communication with the graphical interface. The converter converts each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values. The sequence of values corresponds to the sequence of discrete graphical choices. The apparatus includes a codeword generator in signal communication with the converter. The codeword generator produces a sequence of codewords by applying a decoding function of an error correcting code to each value in the sequence of values. The apparatus includes a security calculator in signal communication with the codeword generator. The security calculator calculates a security value of a security parameter from the sequence of codewords. The apparatus includes a comparator in signal communication with the security calculator. The comparator compares the security value of the security parameter to a threshold value.

[0030] In one embodiment, the security parameter is entropy, and in another embodiment, the security parameter is minentropy. In one embodiment, the apparatus also includes an offset calculator in signal communication with the comparator. The offset calculator calculates, if the security value of the security parameter meets or exceeds the threshold value, an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets. The apparatus, in one embodiment, also includes a hasher in signal communication with the comparator, the hasher applies a hash function to the sequence of codewords to produce a hash of the sequence of codewords if the security

value of the security parameter meets or exceeds the threshold value. In one embodiment, the apparatus also includes a memory element in signal communication with the offset calculator. The memory element stores the sequence of offsets for use in authenticating a user. In another embodiment, the memory element is in signal communication with the hasher. The memory element stores the hash of the sequence of codewords for use in authenticating a user.

[0031] In general, in another aspect, the invention relates to an apparatus for establishing a secret to authenticate a user. The apparatus includes a graphical interface capable of receiving graphical input. The graphical interface receives a secret pattern as graphical input. The secret pattern includes a sequence of discrete graphical choices. The apparatus includes a converter in signal communication with the graphical interface. The converter converts each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values. The sequence of values corresponds to the sequence of discrete graphical choices. The apparatus includes a codeword generator in signal communication with the converter. The codeword generator produces a sequence of codewords by applying a decoding function of an error correcting code to each value in the sequence of values. The apparatus, in some embodiments, includes an offset calculator in signal communication with the codeword generator, the offset calculator calculates an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets. The apparatus, in some embodiments, includes a hasher in signal communication with the codeword generator. The hasher applies a hash function to the sequence of codewords to produce a hash of the sequence of codewords.

[0032] In one embodiment, a discrete graphical choice in the sequence of discrete graphical choices is a selected point on the graphical interface. In another embodiment, the apparatus also includes a point generator in signal communication with the graphical interface. The point generator highlights a plurality of points on the graphical interface as alternative graphical choices for each discrete graphical choice in the sequence of discrete graphical choices. In another embodiment, the apparatus also includes a memory element in signal communication with the graphical interface. The memory element containing a plurality of images and a sequence of images. The receipt of a discrete graphical choice in the sequence of discrete graphical choices triggers the graphical interface to display the next image in the sequence of images from the plurality of images contained in the memory element.

[0033] In one embodiment, the apparatus also includes a training logic element in signal communication with the graphical interface. The training logic element prompts a user to enter a match pattern upon receiving the secret pattern. In one embodiment, the training logic element causes the graphical interface to display the first image in the sequence of images. In one such embodiment, the match pattern is a sequence of match points. In one embodiment, the apparatus also includes a comparator in signal communication with the graphical interface. The comparator compares the match pattern to the secret pattern. In one embodiment, the training logic element causes the graphical interface to highlight the selected point associated with the image on the graphical interface. This may happen during or