

protected form and that also can tolerate some corruption in subsequent readings. Here, Applicants describe methods and systems for applying fuzzy commitment to visual authentication data entry such that the visual authentication data can be stored in a protected form and also tolerate some differences in subsequent readings. Methods for user enrollment and authentication are presented, as well as implementing apparatus.

[0018] In general, in one aspect, the invention relates to a method for establishing a secret to authenticate a user. The method includes receiving on a graphical interface a secret pattern including a sequence of discrete graphical choices. The method includes converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, such that the sequence of values corresponds to the sequence of discrete graphical choices. The method includes selecting a codeword associated with an error-correcting code for each value in the sequence of values to generate a sequence of codewords. A security value of a security parameter is calculated from the sequence of codewords and compared to a threshold value.

[0019] In one embodiment, the security parameter is entropy. In another embodiment, the security parameter is minentropy. In one embodiment, the method also includes rejecting the secret pattern if the security value of the security parameter does not meet or exceed the threshold value. In another embodiment, if the security value of the security parameter meets or exceeds the threshold value, the offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords is calculated to generate a sequence of offsets, and the sequence of codewords is hashed to produce a hash of the sequence of codewords. In another embodiment, the method also includes storing the sequence of offsets for use in authenticating a user. In another embodiment, the method also includes storing the hash of the sequence of codewords for use in authenticating a user. In another embodiment, the method also includes transmitting the hash of the sequence of codewords to an authentication device for use in authenticating a user.

[0020] In general, in another aspect, the invention relates to a method for establishing a secret to authenticate a user. The method includes receiving a secret pattern on a graphical interface that includes a sequence of discrete graphical choices. Each discrete graphical choice in the sequence of discrete graphical choices is converted into a value to produce a sequence of values corresponding to the sequence of discrete graphical choices. A codeword from an error-correcting code is selected for each value in the sequence of values to generate a sequence of codewords. The offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords is calculated to generate a sequence of offsets. The sequence of codewords is hashed to produce a hash of the sequence of codewords.

[0021] 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 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.

[0022] In one embodiment, the method also includes prompting a user by displaying one of the plurality of images on the graphical interface; and receiving a match pattern on the graphical interface for comparison with the secret pattern. In a related embodiment, the match pattern comprises a sequence of match points.

[0023] In one embodiment, the method also includes, during or after the step of receiving the match pattern on the graphical interface, the step of displaying the selected point associated with the image on the graphical interface. In another embodiment, during or after the step of receiving the match pattern on the graphical interface, a line from a match point to the selected point associated with the image on the graphical interface is displayed. In another embodiment, at least one memory cue is provided by presenting the memory cue in response to a point on the image on the graphical interface being highlighted. In another embodiment, a first icon from a plurality of icons is associated with a first point on the image on the graphical interface by displaying the first icon in response to the first point being highlighted, and a second icon from the plurality of icons is associated with a second point on the image on the graphical interface by displaying the second icon in response to the second point being highlighted.

[0024] In one embodiment, the method includes highlighting, for each discrete graphical choice in the sequence of discrete graphical choices, a plurality of points on the graphical interface as alternative graphical choices. In another embodiment, the sequence of offsets are stored for use in authenticating a user. In another embodiment, the hash of the sequence of codewords is stored for use in authenticating a user.

[0025] In general, in another aspect, the invention relates to a method for authenticating a user. The method includes receiving an input pattern including a sequence of discrete graphical choices on a graphical interface. Each discrete graphical choice in the sequence of discrete graphical choices is converted into an input value to produce a sequence of input values. The sequence of input values corresponds to the sequence of discrete graphical choices. A sequence of offsets is retrieved, and each input value from the sequence of input values is summed with the corresponding offset from the sequence of offsets to generate a sequence of intermediate values. A codeword is selected from a choice of codewords associated with an error-correcting code for each intermediate value in the sequence of intermediate values, thereby generating a sequence of codewords. The sequence of codewords is hashed to produce a hash of the sequence of codewords. A user is authenticated if the hash matches a stored hash.

[0026] In one embodiment, prior to the authenticating step, a stored hash is retrieved. In one embodiment, prior to the authenticating step, the hash is transmitted to an authentication device. In one embodiment, each input value in the sequence of input values is a binary value of fixed length. In one embodiment, a discrete graphical choice in the sequence of discrete graphical choices includes a selected region on the graphical interface. In one embodiment, a discrete graphical choice in the sequence of discrete graphical choices is a selected point on the graphical interface. In one