

20. A method for authenticating a user comprising the steps of:

receiving an input pattern on a graphical interface, wherein the input pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into an input value to produce a sequence of input values, wherein the sequence of input values corresponds to the sequence of discrete graphical choices;

retrieving a sequence of offsets;

summing each input value from the sequence of input values with the corresponding offset from the sequence of offsets to generate a sequence of intermediate values;

selecting a codeword from a plurality of codewords for each intermediate value in the sequence of intermediate values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;

hashing the sequence of codewords to produce a hash of the sequence of codewords; and

authenticating a user if the hash matches a stored hash.

21. The method of claim 20 further comprising, prior to the authenticating step, the step of retrieving a stored hash.

22. The method of claim 20 further comprising, prior to the authenticating step, the step of transmitting the hash to an authentication device.

23. The method of claim 20 wherein each input value in the sequence of input values is a binary value of fixed length.

24. The method of claim 20 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected region on the graphical interface.

25. The method of claim 20 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected point on the graphical interface.

26. The method of claim 25 further comprising displaying an image on the graphical interface after receiving the selected point on the graphical interface, wherein each discrete graphical choice in the sequence of discrete graphical choices is associated with one of a plurality of images.

27. The method of claim 25 further comprising associating an icon from a plurality of icons with a point on the graphical interface by displaying the icon when the point is highlighted.

28. The method of claim 20 wherein the graphical interface displays a fractal image.

29. The method of claim 20 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected icon from a plurality of icons on the graphical interface.

30. The method of claim 29 wherein the icon on the graphical interface represents a face.

31. The method of claim 20 further comprising the step of allowing access to a resource in response to the step of authenticating the user.

32. The method of claim 31 wherein the step of allowing access to the resource comprises allowing access to at least one of a hardware device, a computer system, a portable computer, a software application, a database, and a physical location.

33. An apparatus for establishing a secret to authenticate a user, the apparatus comprising:

a graphical interface capable of receiving graphical input, the graphical interface receiving a secret pattern as graphical input, the secret pattern comprising a sequence of discrete graphical choices;

a converter in signal communication with the graphical interface, the converter converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

a codeword generator in signal communication with the converter, the codeword generator producing a sequence of codewords by applying a decoding function of an error correcting code to each value in the sequence of values;

a security calculator in signal communication with the codeword generator, the security calculator calculating a security value of a security parameter from the sequence of codewords; and

a comparator in signal communication with the security calculator, the comparator comparing the security value of the security parameter to a threshold value.

34. The apparatus of claim 33 wherein the security parameter is entropy.

35. The apparatus of claim 33 wherein the security parameter is minentropy.

36. The apparatus of claim 33 further comprising:

an offset calculator in signal communication with the comparator, the offset calculator calculating, 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; and

a hasher in signal communication with the comparator, the hasher applying 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.

37. The apparatus of claim 36 further comprising a memory element in signal communication with the offset calculator, the memory element storing the sequence of offsets for use in authenticating a user.

38. The apparatus of claim 37 wherein the memory element is in signal communication with the hasher and wherein the memory element stores the hash of the sequence of codewords for use in authenticating a user.

39. An apparatus for establishing a secret to authenticate a user, the apparatus comprising:

a graphical interface capable of receiving graphical input, the graphical interface receiving a secret pattern as graphical input, the secret pattern comprising a sequence of discrete graphical choices;

a converter in signal communication with the graphical interface, the converter converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values,