

[0141] In a simple embodiment in which the decoding function  $f$  maps any value  $x$  to the nearest codeword  $c$  without limit on its distance from that nearest codeword  $c$ , use of offsets may not be necessary (STEPS 1524 and 1526). Offsets may not be used in an embodiment in which the decoding function  $f$  has unconstrained codewords. For example, in the geometric analogy of FIG. 9, the input value  $x'$  is nearer the codeword  $c_3$  than any other codeword. Thus, if the codewords in FIG. 9 are unconstrained, the decoding function  $f$  selects the codeword  $c_3$  for the input value  $x'$  even without translation by the offset  $\delta$ .

[0142] In a more complex embodiment in which the decoding function  $f$  maps a value  $x$  to the nearest codeword  $c$  provided that its distance from the nearest codeword  $c$  falls within the minimum distance of the error-correcting code, the use of an offset  $\delta$  may be useful. In this embodiment, a decoding function  $f$  with constrained codewords is used.

[0143] Referring again to geometric analogy of FIG. 10, the decoding function  $f$  will select the included codeword  $c$  for all values within the dotted line circles surrounding each of the codewords  $C \{c_1, c_2, c_3, c_4\}$ . The decoding function will not select the included codeword  $c$  for any value outside the dotted line circle surrounding the codeword  $c$ , even if the value outside the dotted line circle is closer to the enclosed codeword  $c$  than to any other codeword. For example, the value  $x$  in FIG. 10 does not fall within the boundaries of an area that will map to any codeword  $c$ . Nonetheless, embodiments of the enrollment process may select a codeword  $c$  for the value  $x$  at random from the set of codewords  $C$  associated with the given decoding function  $f$ . If codeword  $c_2$  is selected for value  $x$  randomly, then the offset  $\delta$  between  $x$  and  $c_2$  can be represented as (u+470, v-395).

[0144] Referring to FIG. 16, a geometric analogy to the authentication process, which corresponds to the FIG. 10 geometric analogy to the enrollment process, is illustrated. In FIG. 16, an input value  $x'$  is translated by the offset  $\delta$  represented as (u+470, v-395) in the authentication process. When the input value  $x'$  is close to value  $x$  from the secret pattern, the codeword  $c_2$  associated with the value  $x$  can be matched by applying the decoding function  $f$  to the intermediate value  $i$ , generated by translating the input value  $x'$  by the offset  $\delta$ . If the intermediate value  $i$  falls within the decoding constraints of the nearest codeword, the decoding function  $f$  selects the nearest codeword for the intermediate value  $i$ . Here, the decoding function  $f$  will select codeword  $c_2$  for the intermediate value  $i$  because the intermediate value  $i$  falls within the constraints of codeword  $c_2$ .

[0145] Referring again FIG. 15, in embodiments of the invention that conceal the sequence of codewords with a hash function  $h$ , a hasher 1440 (FIG. 14) hashes the sequence of codewords (STEP 1570). In one embodiment the entire sequence of codewords is used as a single input to a hash function. In another embodiment each codeword in the sequence of codewords is used as a separate input to a hash function. In either of the foregoing embodiments, the hashing step taken in the authentication process must correspond to the hashing step used in the enrollment process.

[0146] An alternative embodiment compares the sequence of codewords generated during the enrollment process to the sequence of codewords generated from the input pattern during the authentication process. The hashing step (STEP 1570) is not required in such an embodiment. However, this

embodiment has the disadvantage that the unconcealed sequence of codewords generated during the enrollment process may be accessed by an attacker.

[0147] In the authentication step (STEP 1580), the generated hash is compared to the hash that is a stored representation of the visual password or a portion thereof. In one embodiment, the enrollment hash is stored in a memory element 1430 (FIG. 14) associated with the comparator 1450 (FIG. 14) and recovered from the authentication system 1410 itself. In another embodiment, the enrollment hash is recovered by signal communication with a resource 1460 that is not part of the authentication device. In another embodiment, the authentication hash is transmitted to a resource that has access to the enrollment hash. In such an embodiment, the authentication device need not include a comparator 1450. The user is authenticated (STEP 1580) if the hashes match. Successful authentication enables the user to gain access to a resource as described above.

[0148] An attacker with knowledge of the hash and the sequence of offsets alone would be unable to find an input pattern to authenticate himself. On the other hand, if the user 126 (FIG. 14) enters an input pattern that is close to the secret pattern, it is possible for the resulting sequence of codewords to match the sequence of codewords generated during the enrollment process. Accordingly, the user can be authenticated with an input pattern that is close to the secret pattern given the visual password. Speaking generally, the visual password may be viewed as a fuzzy commitment of the secret password.

[0149] Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed.

[0150] For example, in one embodiment, the sequence of codewords generated in STEP 230 of FIG. 2 is manipulated to produce a cryptographic secret. Such an embodiment need not include the step of calculating a security value. A method for generating a cryptographic secret from a visual password includes receiving a secret pattern made up of a sequence of discrete graphical choices on a graphical interface, converting each discrete graphical choice into a value to produce a sequence of values corresponding to the sequence of discrete graphical choices, selecting a codeword from a plurality of codewords associated with an error-correcting code for each value to generate a sequence of codewords, and manipulating the sequence of codewords to produce a cryptographic secret. In related embodiments, the method further includes calculating 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. In embodiments that include calculating an offset, codewords may be selected at random from the plurality of codewords associated with an error-correcting code because the offset can later be used in conjunction with an input pattern to reproduce the randomly selected codeword. Other embodiments apply a decoding function in the selecting step.

[0151] In one embodiment, the manipulating step of the method for generating a cryptographic secret from a visual password, consists of applying a hash function to the sequence of codewords. In a related embodiment, another mathematical algorithm is applied to the sequence of code-