

authenticate himself with two distinct values x_1 and x_2 . The enrollment process of **FIG. 13** applies a stronger notion of binding. A visual password is defined as strongly binding if it is infeasible for any polynomially bounded player to produce a value collision. A value collision is a pair of values x_1 and x_2 that are not close but that nonetheless both produce the same hash of a codeword $h(c_1)$. A pair of values x_1 and x_2 are close if the decoding function f produces the same codeword c_1 from each of the translated values, mathematically denoted as $f(x_1 - \delta) = f(x_2 - \delta)$. In other words, closeness is defined as within the maximum distance allowed by the underlying error-correcting code. This definition of strongly binding subsumes the conventional definition of binding. Strong binding may, of course, also be defined in a conventional commitment scheme by allowing a value collision to include any two values, x_1 and x_2 , that are distinct. Consequently, if the visual password is strongly binding, then the visual password is also simply binding.

[0122] Further, a visual password is strongly binding if the associated hash function h is collision resistant. If an attacker is capable of finding a value collision, then the attacker can find a collision on the hash function h . The length l of the binary bit string created by the hash function h dictates how hard it is to find a value collision. Effectively, l is the parameter that dictates the strength of the binding in a visual password. Under the common assumption that the most effective means of finding a collision in a hash function is a birthday attack whereby pairs of hashes are compared in an effort to find a match, $2^{1/2}$ hashes, or hash calculations, are required to find a match. Hence, a l value of one hundred sixty, which corresponds to the image length of SHA-1, results in a minimum of about 2^{80} calculations to match a hash. A strong binding enrollment process is particularly useful for visual passwords.

[0123] Resilience

[0124] In the context of an error-correcting code, resilience refers to the maximum level of corruption, or number of errors, in a corrupted codeword i with which the decoding function f can reconstruct the codeword c . This is also known as the error correction threshold t of the error-correcting code. The error correction threshold t is bounded by the minimum distance between codewords in the set of codewords C (known as the minimum distance of the code). In the context of a robust visual password, resilience refers to the maximum offset δ of a value x from an associated codeword c with which the decoding function can derive the codeword c from the value x . The resilience of a robust visual password is clearly bounded by the error correction threshold t of the error-correcting code used in its construction.

[0125] Again, since error-correcting codes require that a binary set of codewords C must contain 2^k codewords, k describes the size of a set of codewords C . Thus, a lower k represents fewer codewords and potentially a greater minimum distance of the code which represents a greater potential error-correction threshold t and a greater potential allowable offset δ . A lower k also represents a lower level of security in a robust visual password. Clearly, the resilience of a robust visual password is inversely related to its level of concealment. A robust visual password achieves a tradeoff between resilience and concealment by varying k .

[0126] In general, the larger the coding efficiency k/n , the larger the minimum distance achievable in an error-correct-

ing code. This is logical since coding efficiency k/n is proportional to the redundancy permitted in the code. The value n of an error-correcting code is typically fixed by the particular application. Similarly, k should be approximately 80 to prevent brute-force inversion attacks against the underlying hash function h in a robust visual password. Where the parameters k and n are fixed, there is no straightforward way to determine the most efficient error-correcting code. The design of codes to handle particular parameter sets is a broad area of research described in some degree by classic texts. In general, practitioners resort to tables of the best known codes.

[0127] To get a sense of the level of resilience attainable in a practical setting, consider an application with a n value of 540. A practitioner may use a table of BCH codes, an efficiently computable class of error-correcting codes, and discover an error-correcting code with a k value of 76, a n value of 511, and a correction threshold t of 85 bits. The value of k in the selected error-correcting code offers an acceptable security level for a robust visual password. A set of codewords C with a length of 511 bits may be used if some data from the application is truncated or compressed. Thus, the selected BCH error-correcting code would enable a practitioner to construct a robust visual password that tolerates errors in any value x of up to almost 17% of the component bits.

[0128] Here, each value x has been selected uniformly at random from the set of n -bit binary strings. If a value x were instead drawn from some non-uniform distribution D within the set of n -bit binary strings, then the security level of a robust visual password will be affected to some degree. Some distributions will not result in a significant diminution in the security parameter k , while others will yield a lesser security level. A good security analysis will, in general, require detailed knowledge of the distribution of values in the relevant application. Nonetheless, if a non-uniform distribution D is only slightly non-uniform, only a slight diminution in security will result. Larger diminutions in security can be compensated for by increasing k . Of course, increasing k may reduce the resilience of the robust visual password.

[0129] Similarly, the differences between the original value x and a subsequent value x' have been assumed to be random here. Note, however, that when the differences between the original value x and a subsequent value x' can be correlated, it is sometimes possible to construct a robust visual password that achieve a higher level of resilience than the error correction threshold t of the selected error-correcting code. This is possible because correlations in the differences restrict the number of likely error patterns. If errors tend to occur in sequence, for example, then it is advantageous to use Reed-Solomon codes. Reed-Solomon codes are well-known for their use in the digital recording media such as compact discs, where so-called burst errors are common. An advantage of Reed-Solomon codes is that much progress has been made recently in achieving probable error correction beyond the error correction threshold t for this class of code. In certain cases, it may even be possible to use such codes to achieve good error correction under independence of bits in e .

[0130] **FIG. 14** illustrates a functional block diagram of an authentication system **1410**, a user **126**, and a resource **1460**.