

## ROBUST VISUAL PASSWORDS

### CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to and the benefit of U.S. Provisional Patent Application Ser. No. 60/191,708, which was filed on Mar. 23, 2000; U.S. patent application Ser. No. 09/544,809, which was filed on Apr. 7, 2000; and International Patent Application Serial Number PCT/US00/03522, which was filed on Feb. 10, 2000 and which claims priority to U.S. Provisional Patent Application Ser. No. 60/119,674, which was filed on Feb. 11, 1999, and U.S. Provisional Patent Application Ser. No. 60/137,687, which was filed on Jun. 4, 1999; all of which are incorporated by reference.

### TECHNICAL FIELD

[0002] The invention relates generally to the field of security and authentication and, more particularly, to a system and method for using a graphical interface to authenticate a user.

### BACKGROUND INFORMATION

[0003] Computer-based authentication systems have been used to authenticate users before providing access to computer systems, devices, and physical locations. Such systems typically make use of one or more of something a user has (such as a physical object or token), something the user knows (such as a secret), or a physical characteristic of the person (e.g. fingerprints, retina patterns, etc.).

[0004] Passwords are an example of something a person knows. They are easy to use and conceptually simple. Because they are generally alphanumeric in form and often closely related to words in natural language, passwords are relatively easy for users to remember. Typically, users can rapidly enter them through standard hardware peripherals such as keyboards. Nonetheless, in terms of their security properties, passwords have shortcomings. Typically, users derive their passwords from a limited portion of the lexicons in their native languages, making them easy to guess, particularly in automated computer attacks. An attack in which common passwords are used to guess a password is known as a dictionary attack.

[0005] The vulnerability of passwords in computer systems is becoming increasingly problematic as computing and networking technologies aim to manage increasingly sensitive information. Consumers are beginning to use smart cards and other portable devices to carry digital cash. At the same time, corporations are making sensitive information more available on their networks and are employing digital signatures in committing to legally binding contracts. Hardware devices like smart cards and authentication tokens provide cryptographic authentication for such applications; but typically the cryptographic features of these devices are secured using passwords.

[0006] It is possible to broaden the distribution of passwords that are used in a system, and thereby strengthen the system by assigning randomly generated alphanumeric passwords to users. Even users with the most retentive memories, however, have difficulty remembering more than approximately seven alphanumeric characters. The total

number of such seven character passwords is about  $2^{35} \approx 10^{11}$ , which is too small to provide resistance against an automated computer attack on the password. Strong resistance to automated password attacks requires a password space on the order of about  $2^{70} \approx 10^{21}$ . This space corresponds to random, alphanumeric passwords of sixteen characters in length, which is too long for practical use by most users.

[0007] While users may have difficulty remembering passwords made up of a random alphanumeric strings, particularly if they must remember several such passwords, they may not have as much difficulty remembering other types of information or similar information in other contexts. A few examples of the other types of nonpassword data an individual may routinely remember are historical and personal events, the configuration of rooms in buildings, and the layout of city streets, not to mention the vocabulary and idioms of her native language. Some of that information may remain fixed in her memory over extended periods of time, even without frequent reinforcement.

[0008] A number of researchers have investigated the use of such everyday information in connection with mnemonic systems as a replacement for passwords. One authentication approach exploits the ability of users to recognize faces. To authenticate herself in this system, a user is asked to identify a set of familiar faces from among a gallery of photographs. While conveniently universal, this system has large memory requirements for the storage of the photographs, and has relatively slow data entry time. Another proposed approach is based on the use of routes on a complex subway system, such as the Tokyo subway system, in connection with secrets, suggesting that users could retain relatively large amounts of information in this context. This approach has the advantage of mnemonic naturalness, but has a strong disadvantage in its idiosyncrasy because not all users live in cities with subway systems or use a subway frequently.

[0009] A commercial system produced by Passlogix, Inc. of New York, N.Y. effectively extends the mnemonic approach by allowing users to select from a range of mnemonic systems. Users can, for instance, choose to use an interface displaying a room containing a collection of valuables, and encode a password as a sequence of moves involving the hiding of these valuables in various locations around the room. This method of password entry appeals to a natural mnemonic device because it resembles the medieval system of the "memory palace," whereby scholars sought to archive data mentally in an imagined architectural space. By allowing the user to select a password herself, however, this approach is vulnerable to the problem of predictability that occurs with conventional password systems. Some passwords are more popular than others, since they are easier to remember. In one example, one-third of user-selected passwords could be found in the English dictionary. Similarly, in a mnemonic system, users are more likely to pick some sequences than others. In one example, a mnemonic system allows users to trade stocks; typically, the users will choose from among the most popular stocks, as these are the easiest to remember. In seeking to guess a password in this system, an attacker is likely to gain a substantial advantage by choosing Dow Jones stocks. In principle, if user passwords are formed as sufficiently long random sequences of moves, a mnemonic system will provide an adequate level of cryptographic security. Typically,