Enhanced Password Processing Scheme Based on Visual Cryptography and OCR

OBJECTIVE:

Main objective of the system is we suggest enhanced password processing scheme based on image using visual cryptography (VC).

ABSTRACT:

Traditional password conversion scheme for user authentication is to transform the passwords into hash values. These hash-based password schemes are comparatively simple and fast because those are based on text and famed cryptography. However, those can be exposed to cyber-attacks utilizing password by cracking tool or hash-cracking online sites. Attackers can thoroughly figure out an original password from hash value when that is relatively simple and plain. As a result, many hacking accidents have been happened predominantly in systems adopting those hash-based schemes. In this work, we suggest enhanced password processing scheme based on image using visual cryptography (VC). Different from the traditional scheme based on hash and text, our scheme transforms a user ID of text type to two images encrypted by VC. The user should make two images consisted of subpixels by random function with SEED which includes personal information. The server only has user's ID and one of the images instead of password. When the user logs in and sends another image, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate user by comparing extracted ID with the saved one. Our proposal has lower computation, prevents cyber-attack aimed at hashcracking, and supports authentication not to expose personal information such as ID to attackers.

INTRODUCTION:

User authentication in general systems has proceeded basically through verification of the ID and password. In order to send and verify password, the system uses a hash-based password scheme that transforms original password to hash value by famed function. The advantages are that it can be adapted in system without difficulty, and computational velocity of process is fast because a type of hash-based scheme is fundamentally based on text utilizing popular hash function such as MD5, SHA256. But it is vulnerable to attacks such as brute force attack or dictionary-based attack plainly by password cracking tool or hash-cracking online sites. Assume that someone defines password "1qaz2wsx" in a system. If an attacker is aware of the hash value " 1c63129ae9db9c60c3e8aa94d3e00495", the value can be sufficiently cracked simply by free crack site . Even though the attacker doesn't know any information about hash function, he or she can easily guess which kind of hash function is adapted in the system. As the result, the attacker can cause secondary damage to the system.