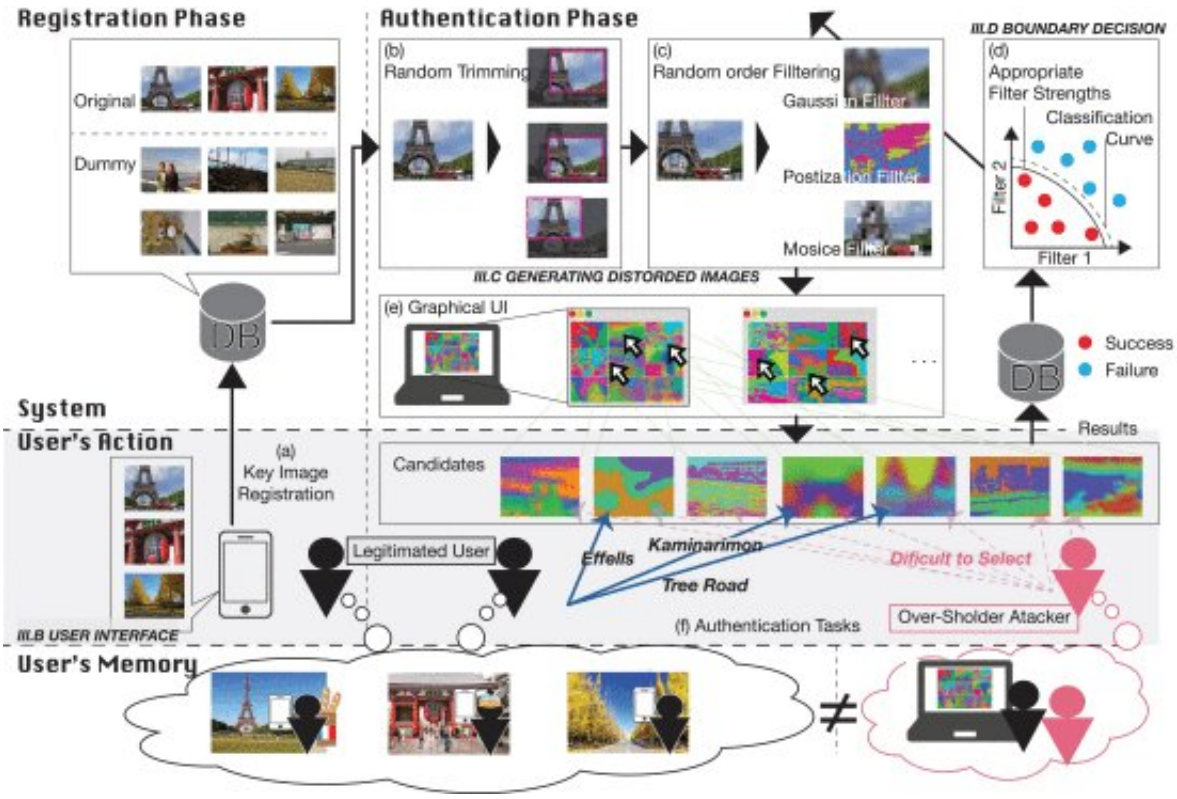
New system for protecting picture passwords using adjustable distortion

March 24 2022



System Configuration and user interface of EYEDi: (a) First, a legitimate user registers several key images from his or her mobile device or PC. In our experiment, the number of key images was five. For simplification, this illustration shows three key images. The key image is stored in a database, and the experimenter prepares a dummy image in advance. (b) The key image is randomly cropped to a size of 4/5. Crop processing makes it difficult for the attacker to find the cue since the feature points in the key image appear and disappear with each authentication. (c) Three image processing filters, Gaussian, Posterization, and Mosaic, are randomly applied to the key image. (d) The strengths of the three filters are calculated from the classification curve

estimated from past authentication data. (e) The key images and dummy images distorted by cropping and filtering are presented on the authentication screen in random order. (f) The user selects the key images from the screen to authenticate. The legitimate user will recall many key image features using familiar memories of these key images as cues. Attackers can record all the selected images by camera recording the authentication screen of a legitimate user. The attacker tries to break through the authentication based on the features contained in the recorded images but cannot find the key image due to the loss of feature points caused by cropping and various distortion changes. Credit: IEEE Access (2022). DOI: 10.1109/ACCESS.2021.3138093

Scientists from the Faculty of Engineering, Information, and Systems at the University of Tsukuba propose an alternative to text passwords using an improved graphical authentication method. By randomly distorting the key images differently each time, the system is much more secure against password crackers, even if they can see the user's screen. This work can lead to significant improvements in internet security.

Although text passwords are a mainstay of a modern life on the internet, they represent a major vulnerability in the global Internet. To remember them, people often choose passwords that are too simple, and may be easily cracked by bad actors. One proposed solution is to instead use a set of pictures, called "key images." To log in, the user choses his or her secret key images from a lineup of pictures. While easy to remember and relatively secure, this approach is still susceptible to what are called "over-the-shoulder attacks," in which someone is watching the screen. Thus, a new approach is needed to help make graphical authentication more resistant to these vulnerabilities.

Now, researchers from the University of Tsukuba have introduced the "Estimating Your Encodable Distorted images" (EYEDi) system. EYEDi works by generating distorted versions of key images during each log-in

by applying several image processing filters. Even if the computer has been compromised with a screen-capture program, which allows a hacker to see the user's screen, they would still not be able to discern the original key images. "Although some previous image distortion methods have been proposed, these methods cannot prevent camera recording or screen-capture attacks, because the key images are the same each time," author Professor Keiichi Zempo explains.

To register using the EYEDi system, five key images are chosen. Then, to log in, a 5x5 grid of images is displayed. Key images are randomly cropped and distorted with a different filter each time. The team tested the system with 20 users over the course of 300 simulated screenshot attacks, using a camera looking over their shoulder. They found that EYEDi prevented hacking better than previous graphical methods. The system can also dynamically adjust the strength of distortion to make sure only authorized users can log in. "Humans are very good at recognizing prominent features of their chosen key images, even with random distortion filters applied," author Professor Keiichi Zempo says. This research may help secure websites as graphical authentication becomes more widespread.

More information: Takayuki Kawamura et al, EYEDi: Graphical Authentication Scheme of Estimating Your Encodable Distorted Images to Prevent Screenshot Attacks, *IEEE Access* (2022). DOI: 10.1109/ACCESS.2021.3138093

Provided by University of Tsukuba