ABSTRACT
Computer security is a critical issue with modern information systems which hold data about related entities such as citizens, employees, employers, corporations, and government agencies. Password authentication has become a widely recognized element of computer security practices where human users are proven or confirmed as legitimate users for access to secure systems. Every user needs to recall its password correctly before access can be granted to an intended system. Remembering the secure password chosen from mixture of random alphanumeric and non-alphanumeric characters is an everyday problem for all users because of individual memory limitation. In an effort to solve this problem, this thesis focuses on knowledge-based authentication to examine the password problems. In this research, more attention will be focused on graphical passwords to improve users’ memory limitations and ability. We start by embarking on literature review of the existing schemes with specific focus on security and memorability. The main research question, therefore, is: “Can graphical password schemes be employed to achieve better memorability and security than conventional text-based password authentication scheme? Empirical studies which involve lab and field studies will be conducted to identify areas of memorability and security improvements. Design and evaluation of new system(s) with several novel design features will be made for memorability and security analysis and confirmation.

KEYWORD
user authentication, password, computer security, usability