# Title: A Secure Child-Friendly Graphical Password Scheme

In an era where children are navigating the complexities of the online world, the need for a child-friendly graphical password scheme becomes evident. Traditional alphanumeric passwords are not only cumbersome for young users but may compromise their online safety. This project seeks to bridge this gap by creating an engaging and secure authentication process that not only educates children on digital security but also contributes to their overall online safety.

**Objective:**

Develop a graphical password scheme tailored for applications designed for children, ensuring the authentication process is both entertaining and effective. The scheme should exhibit resistance to guessing and shoulder surfing attacks.

**Literature:**

In the literature, there are several graphical password schemes proposed such as PassFaces, DejaVu or other schemes [1] that use facial images, items, and random images to log users in as shown in Figure 1.

A collage of people's faces

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Figure 1: Some example graphical password schemes.

However, these schemes are not designed for children and turned out to be hard to use for adults as well.

**Project Components:**

To address gaps in the literature, you need to do the following:

**Graphical Password Creation Interface:**

Design an intuitive and visually appealing interface allowing children to create their graphical passwords. Do some research on children-friendly user interfaces and applications.

**Implement the registration phase and the login phase:**

In the registration phase, you need to define the process of how the user can register for a service by selecting their graphical passwords. Similarly, you have to define the process of a login phase, when the system needs to verify if the given graphical password is the correct one. Graphical passwords are different from textual passwords and require extra considerations. You can read the paper [1] and other related research to find out more about how researchers implement this phase. Existing graphical passwords usually require several rounds of picture selections.

**Security:**

Incorporate an algorithm or procedure for selecting passwords (e.g., number of pictures or items selected by the user per number of total pictures and items) that ensures a sufficient level of security to resist guessing and shoulder surfing attacks.

**Programming Language:**

You are allowed to use any programming language of your choice as far as it supports a graphical interface.

**Testing and evaluation:**

Design and propose a test plan to test the usability and security of the proposed password scheme. You should also implement secure storage of the graphical passwords.

**References**

[1] Xiaoyuan Suo, Ying Zhu and G. S. Owen, "Graphical passwords: a survey," 21st Annual Computer Security Applications Conference (ACSAC'05), Tucson, AZ, 2005, pp. 10 pp.-472, doi: 10.1109/CSAC.2005.27.