

Authentication System For University Student Portal Using Images

Haitham Al-Sinani

Course Code: B382, Student ID No: 304910

Supervisor: Mr. Chi, Moderator: Dr Branislav

Location: A2.2

Problem Specification and Objectives

Nowadays, the number of online services requiring their users to authenticate using passwords continues to rise sharply. This causes the number of passwords needed to also rise! For certain applications, research suggests that the use of images may be a more effective combination of security and ease of use.

The project is to explore the strengths and flaws of an authentication system that uses random art images for use by University students accessing their portals. This requires 3 main steps:

1. Implement an experimental authentication system, called H-IBAS-H, that uses image-based keys.
2. Test the experimental system by conducting surveys with real users.
3. Analyze the strengths and weaknesses of image-based authentication using the experimental results.

1. H-IBAS-H

1.1 Primary user

H-IBAS-H is designed primarily to be the login system that authenticates the University students to their portals.

1.2 Authentication Algorithm

The pass-images are randomly distributed on the login rounds. Therefore, every round may have all, some or none of the pass-images. At least, one login round must contain no pass-images.

1.3 H-IBAS-H modes

Pre-set mode

The H-IBAS-H administrator is responsible for setting the number of the pass-images and the number of the training and the login rounds that the student may go through. The system admin is free to set any number that they believe it is suitable. Currently, the pre-set mode sets H-IBAS-H to operate as follows: The students may select 4 pass images from the offered 21 images and they may go through at least 2 successful training rounds. The students are free to train more if they wish. When they log in, the students may go through 4 login rounds. The students can have 3 attempts to retry to log in before their account gets locked. However, if their account gets locked, the legitimate student can check their email where they will find a reactivation link that enables them to reset their pass-images. Another scenario where the students forget their pass-images, they can click on the "forgot pass images" link where they enter their user name and a reactivation link is e-mailed to them.

Flexible mode

All the features included in the pre-set mode are also applicable here but the difference is that, it is the student who can decide on the number of pass images, not less than 2, they want to use and the number of the login rounds, not less than 2, they want to go through. The student can also go through as many times of training rounds, not less than 1, as they wish. This mode is primarily designed to provide full flexibility to the students.

2. Experiments

In all of the experiments, the participants were invited to authenticate with H-IBAS-H and were afterwards asked to fill in a questionnaire.

2.1 First Experiment (Pilot Survey)

This was an initial study that aimed to solve any ambiguities in the user questionnaire and to improve H-IBAS-H to be as much user-friendly as possible.

2.2 Second Experiment

Some of the objectives of this experiment are shown below:

- To find out the reasons behind the users' choices of their pass-images.
- To assess the time consumed while registering and logging with H-IBAS-H.
- To assess the ease of use.
- To obtain the users' opinions as in where H-IBAS-H stands in comparison with other authentication systems in terms of speed, ease of use and e joy of use and many more.
- To find out the reasons behind the inability, by some users, to either register or to authenticate.

2.3 Third Experiment (4-week Experiment)

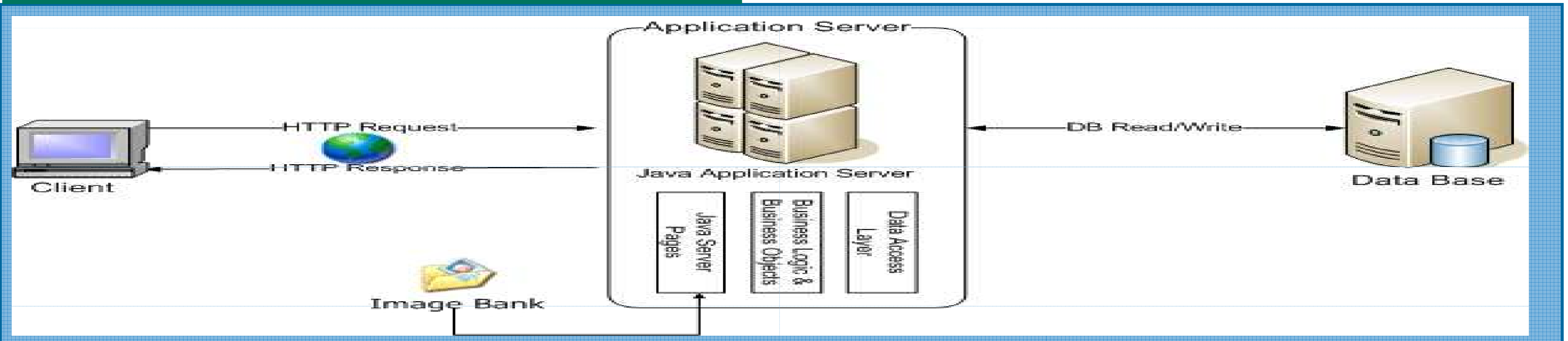
This experiment was run over a period of 4 weeks.

- Some of the objectives of this experiment are shown below:
- To inspect whether the number of experiences with H-IBAS-H has an effect on the participants' answers.
- To examine the effects of updating the students' pass-images after becoming familiar with the old ones in terms of whether the new pass-images would be confused with the old ones.
- To study the effects of having more than one image-set.
- To evaluate the participants' ability to recognise their images over a 4-week period.

3. Findings

- The flexibility in key generation should be provided if an image-based authentication system is desired to gain high success in usability.
- The similar images should be eliminated if an image-based authentication system is desired to score a high percentage of success in usability.
- Authentication stability can be provided even where the image-based authentication system is not frequently used.
- Image-based systems that use random art as their authentication keys depend on recognition as well as recall.

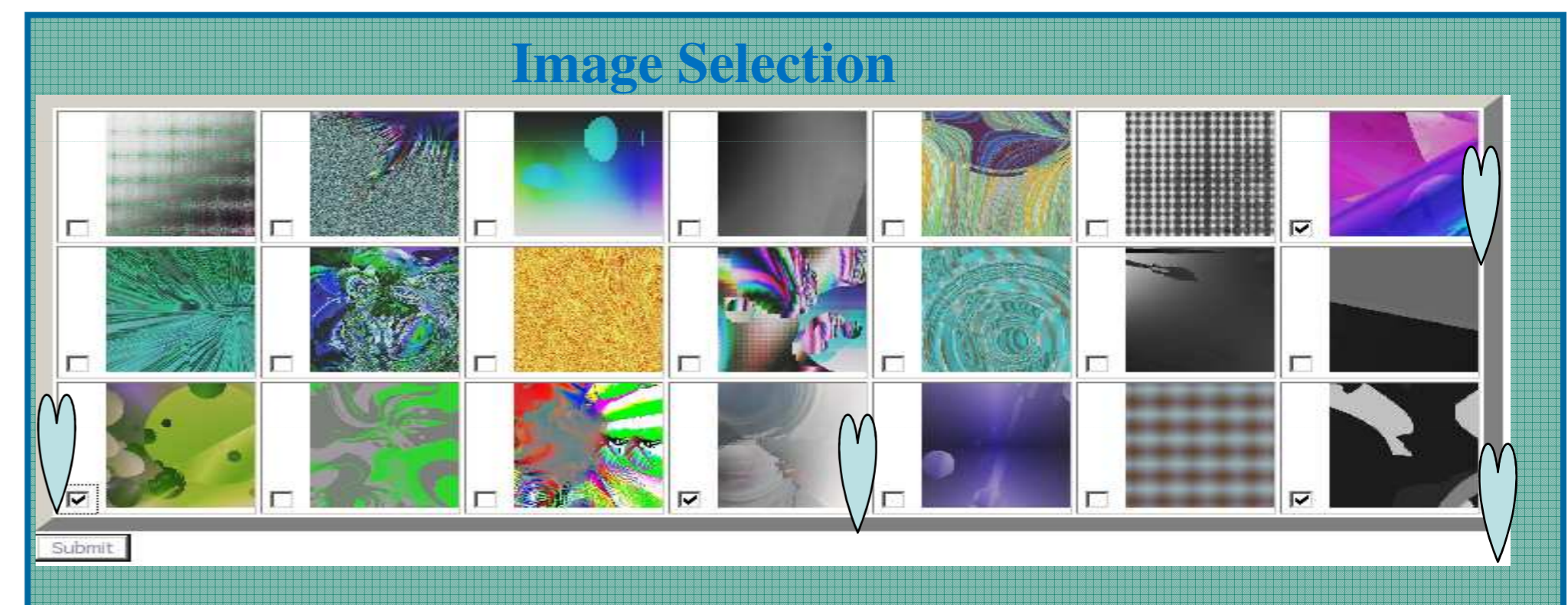
Physical Application Architecture



Success in the 2nd experiment

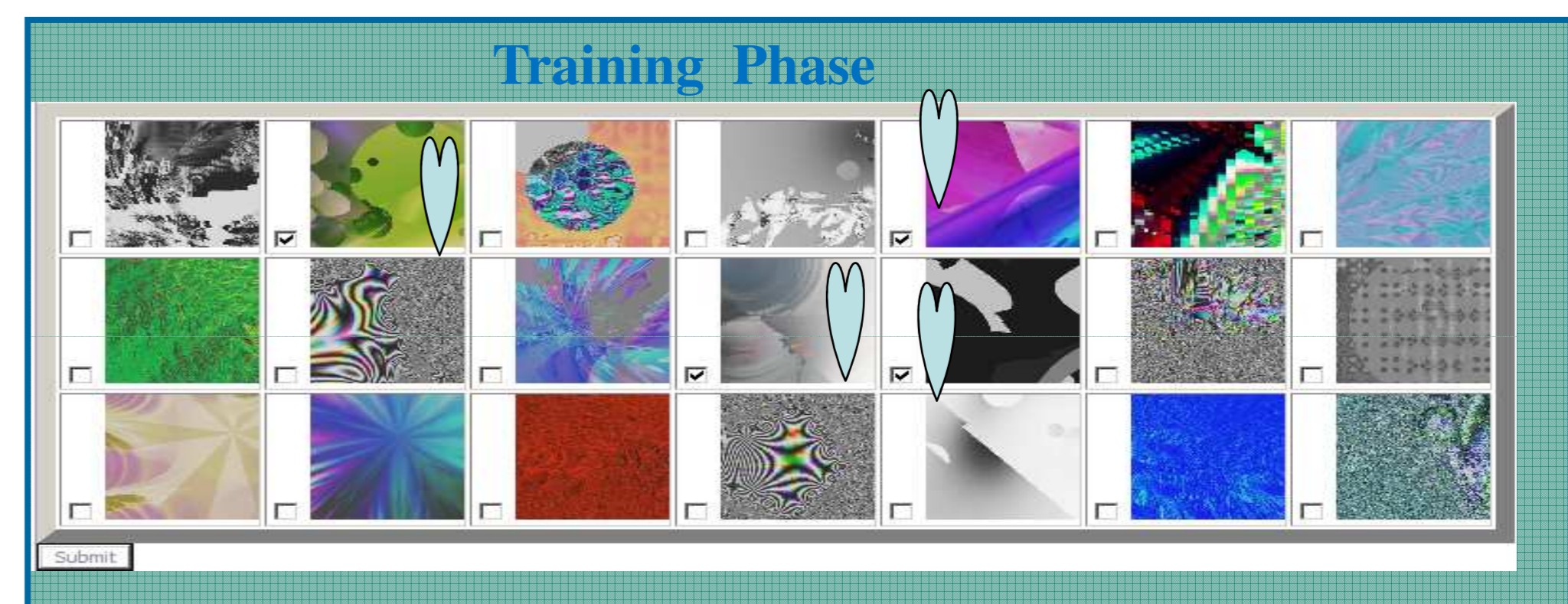
	Successful (%)	Successful participants	Total participants
Registration	98.6%	69	70
authentication	95.6%	66	69

Phases of H-IBAS-H



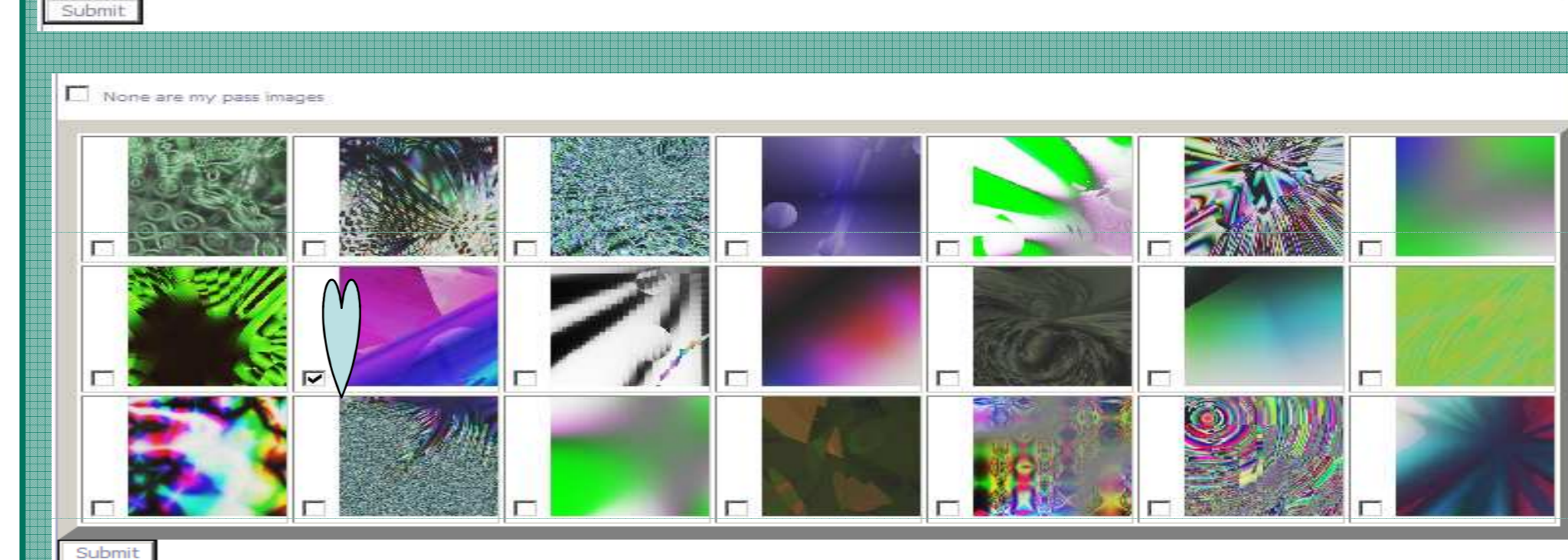
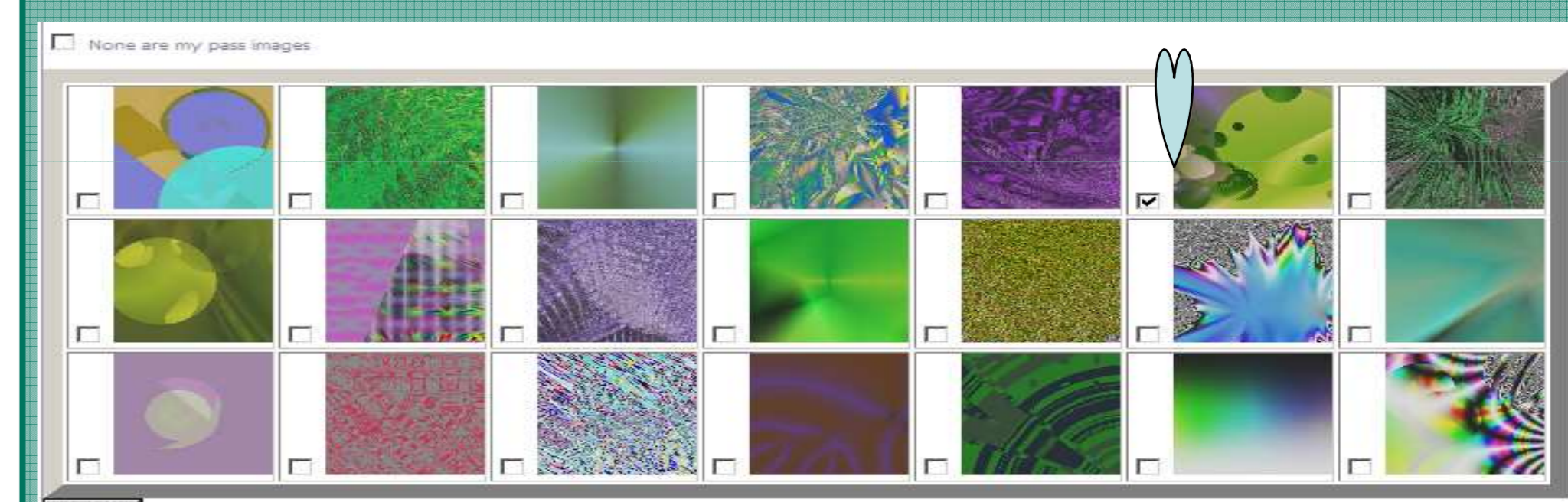
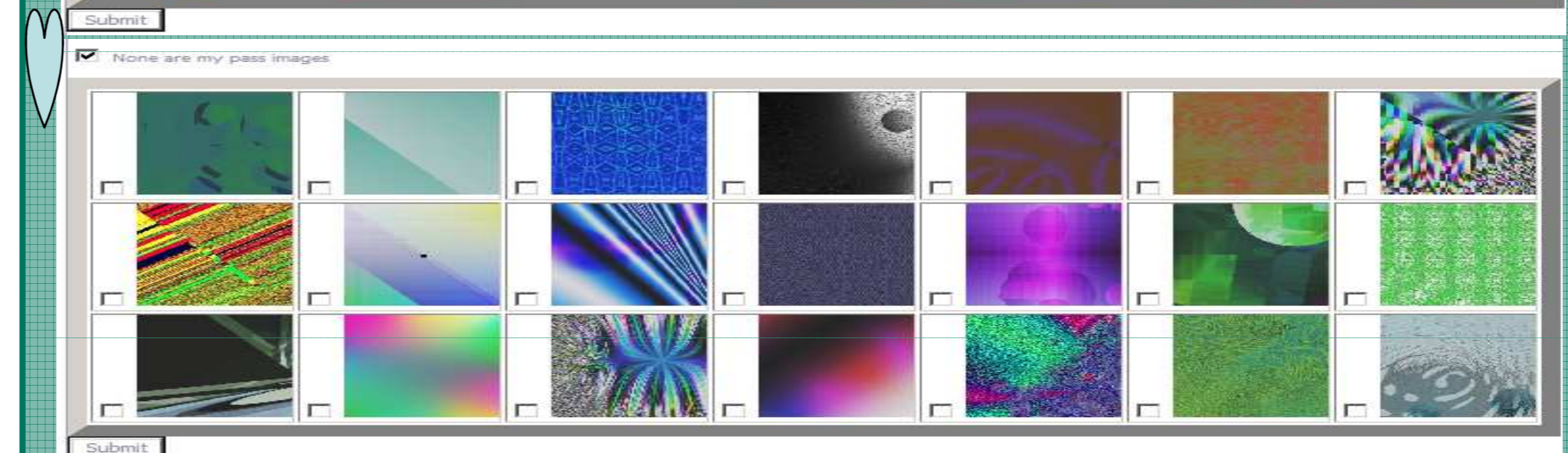
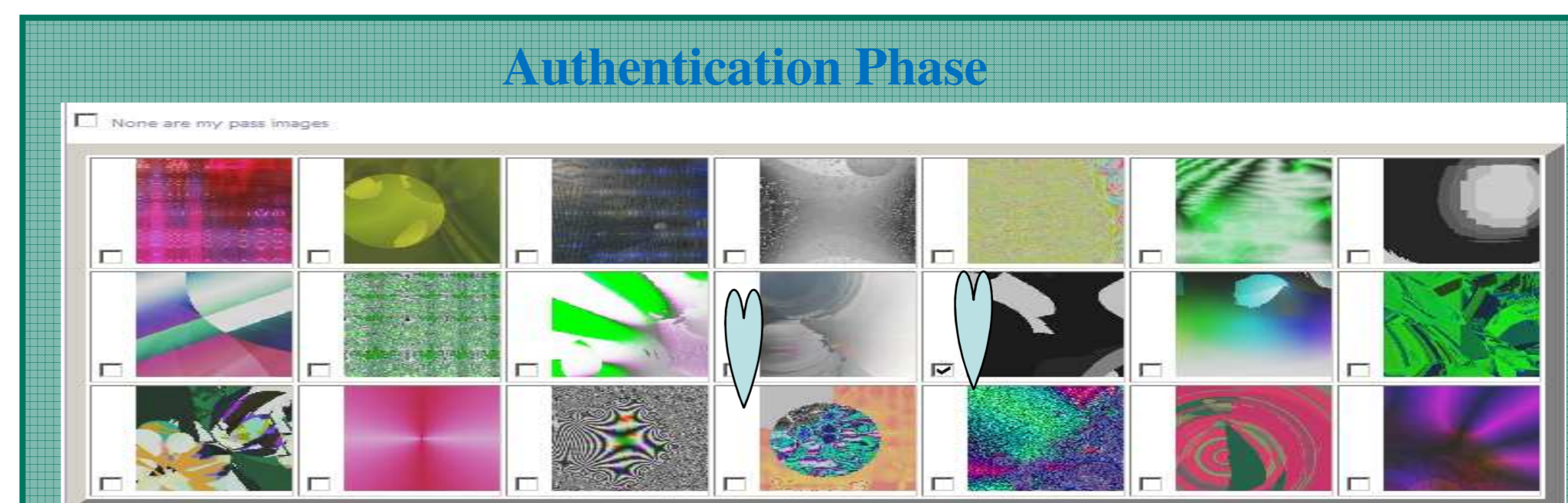
Success in the 4-week experiment

Week	Successful logins (%)	Successful participants	Total participants
1	100%	20	20
2	80%	16	20
3	100%	16	16
4	93.8%	15	16



Success after the pass-images were updated

Week	Successful logins (%)	Successful participants	Total participants
3	100%	16	16
4	75%	12	16



4. Conclusion

The high rate of success, achieved by users attempting to authenticate with H-IBAS-H, strongly supports the arguments of those seeking to push image recognition forward as a viable alternative to the widely-used text-based systems.