A Serious Game on Image Steganography Training for Students in Higher Education.

JESPER SIMON, University of Twente, The Netherlands

As the world becomes more digital and we spend more time online, our risk of falling victim to cybercrime increases. Nowadays, a popular technique used by cybercriminals is steganography; due to it being hard to detect. When using steganography, malicious data is hidden in non-secret harmless-seeming media. The type of steganography most commonly used by criminals is image steganography. When an image is opened or downloaded it executes a script locking someone their computer for ransom or other malicious intent. Cybersecurity training is needed to spread awareness about the risk of image steganography attacks. Gamification has been shown to be an effective tool in designing cybersecurity training tools. However, a gamified training tool on the cybersecurity topic of image steganography has not been developed. In this research, we develop a novel serious game. Engagement is shown to have a positive effect on motivated learning and knowledge retention. Therefore we identify gamification techniques that increase engagement with the game, like levels, rewards, and feedback. The training tool is an Angular web application with TypeScript and HTML as its programming languages. To prove the effectiveness of the proposed tool in engaging its user and being a helpful tool in cybersecurity training a remote experimental study is performed. 15 university students from the Netherlands aged 18 to 24 have taken part in this study. Next to using the tool, participants also fill out two surveys; one prior to using the tool about their background knowledge of steganography and cybersecurity in general, and one after using the tool on their experience playing the game. The results are analyzed effectively which indicates that the users enjoyed learning via the game, and felt that they would be motivated by improving some key elements of the game. Future work seeks to extend the tool by adding more engaging questions covering a range of security techniques on steganography.

Additional Key Words and Phrases: Image steganography, Serious games, Steganography awareness tool, Cybersecurity training, University students

1 INTRODUCTION

People spend over 40% of their waking life online [20]. That is an increase of more than 5% over the last decade . This increase in online presence also increases an individual's risk of falling victim to cybercriminal activity. In the Netherlands, as traditional crime has decreased [27], the number of victims of cybercrime has steadily increased over the years [26, 28]. Every year the number of victims of cybercrime has steadily increased from 1.2 million in 2018, to 2 million in 2019, to 2.5 million in 2021. The consequences of these crimes are often not only financial problems but also emotional and mental problems.

To protect our private information when online, cryptography has been developed. Which is defined as the science or study of the techniques of secret writing, especially code and cipher systems, methods, and the like [10]. Most people are aware of the practice and its applications in daily life. For example, making an online purchase or sending a message via WhatsApp or Telegram. Cryptography secures this information by converting it into unintelligible text using different techniques like encryption and hashing, which makes it hard for hackers to hack into your system without knowing the code used for security [46]. Without cryptography our personal information and secrets would all be out in the open [34].

The encrypted data that is created using cryptography is useless to cybercriminals. Therefore, they try to trick people in sharing their non-encrypted data. Phishing [47] is a known technique used by cybercriminals in which an attacker tries to gain sensitive personal data by sending an e-mail containing a link to a fake/malicious website or an infected file [3]. In the study of Cuchta et al. [9], a substantial proportion of the university population surveyed, approximately 40%, were susceptible to phishing emails, and roughly 20% were duped by spoofing tactics, leading to the submission of their login credentials on a counterfeit login page. This shows that the human element poses a substantial risk in the realm of cybersecurity. Therefore, it is very important that individuals are trained properly about the risks they might face when being online. Cybersecurity training is an effective tool in preventing cyber attacks prompted by this human risk factor.

However, instructor-led training is often expensive, and online training tools often lack the ability to engage their users, which results in less effective training. A popular tool to promote user engagement is **gamification** [33]. In gamification, common game play components (such as point scoring, competition with other players, and game rules) are added to other types of activities like a progress bar for filling out your user profile, adding badges for completing exercises in gamified education, or in this case to promote engagement with the training content and improve the learning efficacy [25]. In game-based learning the training as a whole is turned into a **serious game** [49]. A serious game is a tool used in game-based learning with the only goal of effectively teaching about a specific topic. Serious games have been developed as effective training tools that cover cybersecurity topics like safe passwords, updating software, and phishing [15, 29, 40]. Quiz games enhance the 'testing effect', in other words improving learning by requiring users to consistently and repeatedly recall information, leading to better learning outcomes [22]. In section 2.1.2 further research is done on gamification and serious games.

As more awareness spreads about cybersecurity and the tools and practices on how to keep yourself safe, cybercriminals try to find new and covert ways to trick people. One of the commonly used methods is the obfuscation technique called **Steganography** [50]. Steganography is known as the practice of hiding secret information in data without the victim's awareness. It thereby conceals the existence of a message by substituting unused bits of data in

TScIT 38, February 3, 2023, Enschede, The Netherlands

ordinary files like images, sound, text, audio, and video with other unnoticeable data. Plaintext, ciphertext, and occasionally a picture can all be used as secret data. The technique most frequently used for hiding data in files is to use a visual image as a cover (i.e. image steganography), as images are a popular media for sharing content. An amusing image, meme, or comic can be easily disseminated without considering the potential ramifications. Steganography, unlike encryption, can be challenging to detect and is this often utilized for nefarious purposes. In section 2.1.1 steganography, and especially image steganography, is further explored.

Some training courses are available online on steganography [19, 24]. However, most require some form of payment and none of the training available is gamified. Upon conducting conversations with university students of a technical background I found that only a small percentage of them have heard about steganography. And an even smaller percentage indicated having more in-depth knowledge about the subject. The aim of this study is to develop a novel open-source serious game on the cybersecurity topic of image steganography with the goal of increasing awareness and knowledge among the general public on this topic.

In developing the tool, effective gamification techniques are selected for engaging its user. A thorough evaluation of these techniques is conducted, and a selection is made for incorporation into the game. And lastly, a study is conducted on the effectiveness of the tool in training on the cybersecurity topic of steganography. From the literature in Chapter 2.2, no tools are identified to take into account bias introduced by the participants' state of mind. To mitigate this bias, additional questions are presented to the participants to evaluate their state of mind. These steps give rise to the following research questions.

Main research question
What is the effect of a quiz-based serious game on image steganography with questions set in real-life scenarios on engagement?

Sub research questions

(1) What gamification features have a positive effect on engagement when examining current cybersecurity training and education tools?
(2) Which of the gamification features that were found in subquestion 1 can be applied to a gamified steganography training tool?
(3) What is the effect of a gamified steganography training tool on engagement when implementing the features identified in sub-question 2 on user engagement?

The training tool is an Angular web application using TypeScript and HTML as its programming languages. To determine the effect of the tool on user engagement we perform an experimental study involving 15 university students from the Netherlands aged 18 to 24.

The remaining chapters of this paper are organized as follows. In Chapter 2, literary research is performed on gamification and steganography, as well as related works on gamified cybersecurity training tools. In Chapter 3 the methodology is defined. In Chapter 4 we present our design of the training tool. In Chapter 5 the study results are analyzed. In Chapter 6 conclusions, limitations, and possible future works are discussed.

2 RELATED WORK

In this chapter, an overview of the subjects of steganography, specifically image steganography, and gamification is given. Additionally, previously developed educational and cybersecurity training tools that make use of gamification are explored and their strengths and weaknesses are defined.

2.1 Background Knowledge

When looking at steganography, the definition of steganography, important terminology, common image steganography techniques, and some real-world examples of an image steganography attack are discussed. When looking at gamification, we define the difference between gamification and serious games. For each category, their game elements and main purpose are identified.

2.1.1 Steganography. is the practice of enclosing information in another message or physical item in a way that prevents human inspection from revealing its presence. The term comes from the Greek word steganographia, which combines the words steganós, "covered or concealed", and -graphia, "writing" [36]. A tangible illustration of the concept is the use of invisible ink, which only can be perceived knowing to hold it over a heat source or make it come in contact with a certain chemical. This heat source or chemical can be seen as the key to the message. In the realm of digital technology, we refer to a computer file, message, image, or video that is hidden within another file, message, image, or video in computing and electronic environments, which can only be perceived by knowing the right key.

In phishing e-mails, the infected file is usually in Excel, Word, or PDF format. However, other media, like image, audio, and video files cannot be considered "safe" as these could also contain malicious software [8]. Malicious software that has been hidden by employing steganography is also known as Stegware [52].

In image steganography different image formats have different advantages and disadvantages, and some require other obfuscation techniques than others. Some popular formats used in image steganography include PNG, JPEG, JIFF, BMP, and GIF. Sinha compares the effectiveness of using 'Least Significant Bit' coding, replacing the least significant bit or bits with the secret data, on the PNG and JPEG image formats [37]. This comparison shows that the PNG format is preferable when using LSB coding, because of its characteristic of lossless compression and high data capacity for the secret message. It had been commonly believed that effective steganography could not be performed on JPEG files, because of its use of Discrete Cosine Transform (DCT) in compression [7]. However, this obstacle was overcome by first removing the redundancy of the image, which would otherwise be lost in compression.

When hiding a message in an image by using LSB coding, you would assume the image size to not increase as you are just replacing bits and not adding any. But this theory does not hold for most of the aforementioned image file formats. This is because file sizes depend on the compressed data of an image. This compression relies

on transforming the pixel data using mathematical equations. For example, a repeated block of similar pixels can be represented by a placeholder referring to this sequence of pixels. When hiding a secret message using LSB, you are changing pixel values ever so slightly. Therefore, these blocks of pixels are not similar anymore and thus are compressed using more data. Additionally, when a pixel changes such that an equation does hold, it is compressed using fewer data. The change of the file size does not apply to Bitmap (BMP) files, as they are by definition not compressed [45].

In Table 1, the LSB method is applied to different image file formats, and their characteristics are compared [5, 38, 44]. LSB is explored, as it is the most common method used and is very straightforward to explain. From the table, it can be found that when redundancy is removed JPEG is the most robust file format. However, it has a small payload. BMP has the highest payload, but is little robustness against statistical attacks and image manipulation. PNG is therefore a reasonable midpoint. With better robustness than BMP and a higher payload than JPEG.

Table 1. 'Least Significant Bit' (LSB) steganography applied to different image file formats.

Property \ File type	JPEG	PNG	BMP	GIF
Invisibility	Medium	Medium	High	Medium
Payload capacity	Low	Medium	High	Medium
Robustness against Steganalysis detection	Medium	Medium	High	Medium
Robustness against statistical attacks	High	Medium	Low	Low
Robustness against image manipulation	Medium	Medium	Low	Low
Non-suspicious format	High	High	Low	Medium

Real-world steganography attacks target various parts of society. Kaspersky [41] released a report in June 2020, uncovering deliberate assaults on industrial targets across numerous nations. Here targets opened Excel email attachments containing malicious macros. The macros executed PowerShell scripts, one of which included a command to download specified photos from online image-hosting providers. Each image had additional harmful information concealed in various pixels that, when decoded, allowed threat actors to install Trojans that allowed them to eavesdrop on network traffic or steal passwords. Sansec [43], a Dutch eCommerce security platform, presented research in November 2020 revealing that threat actors have hidden skimming malware into SVG images on eCommerce checkout pages. The attacks utilized a concealed malicious payload contained in SVG images and a decoder located independently on other portions of the websites. Because the graphics were basic logos from well-known firms like Facebook and Google, users inputting their information on the hijacked checkout sites would not detect any anomalous behaviour. Additionally, because the payload was concealed within what looked to be the proper usage of SVG element syntax, common security scanners that look for incorrect syntax were unable to find the malicious activity.

2.1.2 Gamification. has been shown to be an effective strategy in the design of training tools for cybersecurity. Gamification is the use of game-design elements and gaming concepts in a context that is not game-related [13], in this particular instance, the realm of education and training. Gamification is divided into 2 main categories: structural gamification and content gamification (serious gaming) [1]. An overview of the differences between (structural) gamification, game-based learning, and serious games (i.e. content gamification) can be found in Figure 1.

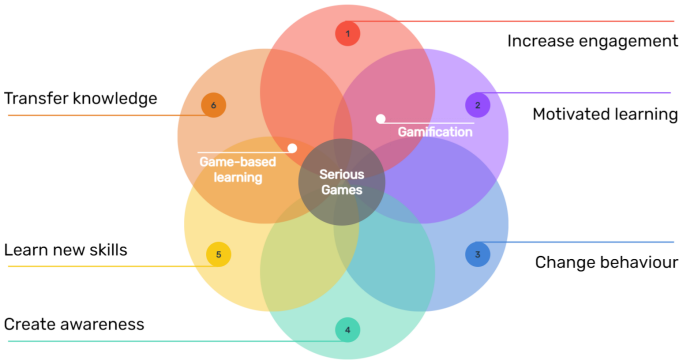

Fig. 1. Difference of Gamification and Serious Games [23].

Structural gamification adds new, dynamic components to existing materials, systems, and processes. Since the gaming material is shown separately from the serious content, the application's existing language and mechanisms are not changed. For instance, a learning app may keep the instructional texts while also adding mini-games between each lesson and prizes for the user as they advance. As a result, although students are still studying the same content, the educational experience has been greatly enhanced through an increase in enjoyment. Some examples of types of structural games are Progression-based games, Badge-based games, Casual games, and Competition games. Duolingo, the language learning app, and RobinHood, the stock trading app, are some well-known examples of structural gamification [21].

Content gamification, also known as serious gaming, is to improve the engagement of existing educational material. By including components like challenges, feedback loops, and storytelling, the curriculum is changed to be more game-like without really converting the training into a game. This method retains the training's focus on the subject while improving the learner's engagement with the information without creating a complex game. Instead of going over the learning goals at the beginning of the course, you may start it with a tale if you are instructing your staff on safety practices during fire breakouts. Then, ask them to put what they've learned into practice by coming up with a tale of their own that illustrates what to do in the event of a building fire [11].

2.2 Training/Educational Tools

When exploring existing gamified cybersecurity training tools, the gamification techniques which are implemented are identified and discussed.

2.2.1 Virtual Escape Room. Williams and El-Gayar [51] explore a virtual escape room as an entertaining medium for collaborative cybersecurity education. This game-based learning experience promotes a good experience while also challenging the participants with problems they need to overcome. Gamification elements used to promote users' motivation and engagement are identified.

- Challenges
- Storytelling
- Rewards
- Time constraint

2.2.2 Capture the Flag. Karagiannis et al. [18] reviews Capture the Flag (CTF) [48] platforms as tools for cybersecurity education. Here gamification is applied by adding game elements to the existing educational content. Each platform is evaluated by a systematic comparative study and an experimental study based on one-one interviews. From the interviews with the participants, some important elements of the platforms were identified for promoting engagement and enhancing the users' experience.

- Rich visuals
- A sense of control
- Hypermedia
- Scoreboards
- Rewards
- Personalization
- Storytelling
- A clear structure
- Challenges

2.2.3 GenCyberCoin. Game components were included in the GenCyber [30] summer program run by Jin et al [17]. They created four serious games: a 2D GenCyber card game, a 3D VR safe online behavior game, a 3D social engineering game, and a cyber tower defense game. Their research showed promising benefits to using games as camp activities. Ford and Siraj [14] built upon the basis of these games and created a web platform employing gamification to further incentivize and engage students with cybersecurity topics during the weeklong GenCyber summer camp. Additional features were added to accomplish this goal.

- Rewards
- Feedback
- Time constraint
- Challenges
- Scoreboards
- Hypermedia

2.2.4 AWATO. Ferro et al. [12] highlight that many popular games with cybersecurity themes put the player in the role of the attacker instead of someone trying to protect a system. In the serious game Another Week at the Office (AWATO), a player takes on the role of a newly hired security analyst who is tasked with finding a variety of vulnerabilities made possible by human error within AWATOcorp. Gamification elements were identified that are key to the design of the game.

- Storytelling
- Feedback
- Challenges
- A sense of control

3 METHODOLOGY

In this chapter the proposed methodology is described. Figure 2 shows a flowchart of the methodology.

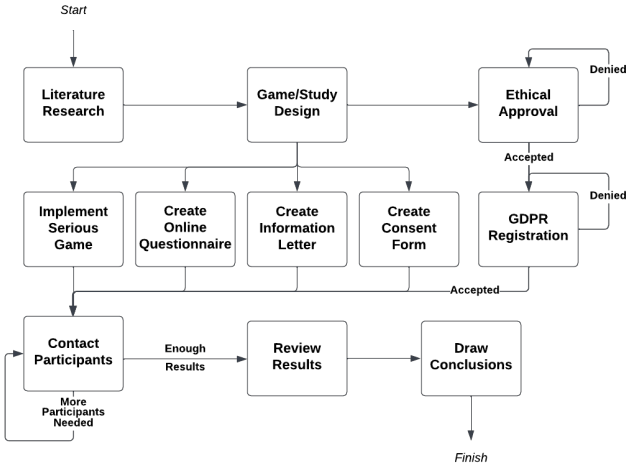

Fig. 2. Flowchart of the methodology.

Literature research is conducted on the topics of gamification and steganography, more specifically serious games and image steganography; this can be found in Chapter 2.1. As a gamified training tool has not been developed before on the cybersecurity topic of steganography, serious games on other topics of cybersecurity are considered; this can be found in Chapter 2.2. Effective gamification strategies are identified and presented in an overview in Table 2.

The tool is designed based on a selection of the identified effective strategies; the design can be found in Chapter 4. This selection is focused on high levels of engagement. The plan for the experimental study is created concurrently. To perform this study ethical approval from the university [35] and GDPR registration [32] are acquired. The next step is the implementation of the serious game. Additionally, three documents are created; the surveys, information letter, and consent form. The information letter informs the participants of the study about the methods that are used to conduct the study, what is expected of them during the study, and what their rights are when it comes to participating in the study.

The training tool is a web application that is hosted online so that participants do not have to download any content to take part in the study and is available on any platform. It is hosted on itch.io [16] which provides free hosting of the game. Qualtrics [31], a platform often used for academic research, is used for conducting both pre-game and post-game surveys.

When the implementation and creation steps are finished and both approval and registration are accepted. To recruit participants for the study, students are personally approached through messaging. The study involves university students from the Netherlands. A study from 2020 shows that students are highly susceptible to cyber

attacks [39]. Students participating in the study are aged 18 to 24 years old. Statistics from the Central Bureau of Statistics (CBS) in the Netherlands show that the demographic with the highest prevalence of cybercrime victims are within this age range [26].

When conducting the study participants are asked to fill out a survey prior to playing the game. In this survey, their background and prior knowledge concerning steganography and cybersecurity are assessed. Afterward, participants play the serious game. After completion of the serious game, a final survey is conducted. This survey is to check the effectiveness of training using gamification. Survey questions inquire about the users' acquired knowledge and the user experience of the tool. From the surveys and game-play conclusions are drawn. The survey data and game data are evaluated quantitatively as well as qualitatively.

4 DESIGN

This chapter describes the goals of the training tool, which elements are implemented into the design of the game, the educational content of the questions, and the structure of the surveys.

4.1 Goals

The main goal of the gamified image steganography training tool is *to increase the players' awareness of image steganography attacks and provide them with the knowledge to identify possible signs which would indicate such an attack*. This includes:

- Conveying attack methodologies that are used by attackers.
- Improving the capability to detect signs of an attack and thus mitigate a possible steganography attack.
- Being able to use the gamified tool without acquired prior knowledge.

To achieve these goals a serious game is designed based on gamification techniques that promote engagement with the content subject and an enjoyable user experience.

4.2 Game Design

An overview of the gamified techniques identified from the training tools explored in chapter 2 can be found in Table 2. From this table, we can identify all gamification components that have a positive influence on user engagement and promotes a better user experience.

In designing our game common game design elements were selected from the available literature. When looking at Table 2, the most common game elements implemented are *Challenges*, *Storytelling*, and *Rewards*. In the training tool challenges take the form of quiz questions, storytelling is applied by telling a story around each question and presenting a real-life application of image steganography, and rewards are implemented by presenting the player with a reward when completing the game.

Table 2. Gamification techniques used in cybersecurity training tools.

Techniques \ Tools	ESCAPE	CTF	GCC	AWATO
Challenges	✓		✓	✓
Storytelling	✓	✓		✓
Rewards	✓	✓	✓	
Time constraint	✓		✓	
Rich visuals		✓		
Sense of control		✓		✓
Hypermedia		✓	✓	
Scoreboards		✓	✓	
Personalization		✓		
Clear structure		✓		
Feedback			✓	

4.2.1 Structure & Categorization. The game is a quiz-like game where your knowledge is tested on the topic of image steganography. Different categories of questions and randomization of the questions as well as the order of the answers are added to stimulate engagement.

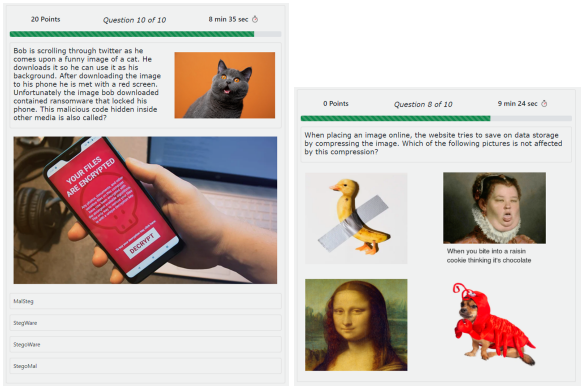

Fig. 3. A multiple-choice question (left) vs. an interactive question (right).

Each instance of the game features 10 questions from a pool of 20 questions evenly divided into 3 question categories. These categories are *Fill in the blank*, *Multiple-choice*, and *Interactive*. This last category exists out of questions where users have to inspect image details and also questions where interaction with image steganography tools is required. In Figure 3, an example of a multiple-choice question and an interactive image inspection question can be seen.

4.2.2 Levels & Scoring. To not demotivate participants by possibly only getting harder questions difficult scaling is implemented. A difficulty level is assigned to each question. There are 4 difficulty levels: easy, medium, hard, and expert. The levels are assigned by hand when implementing a question. Each correctly answered question earns the player 10, 20, 30, or 40 points respectively. When starting the game a person answers a question if they have played the game before; if that is true they enter their starting difficulty level. When playing the game for the first time a person starts at

easy difficulty. When answering a question correctly the difficulty of the next question goes up by one level for each correct answer until it reaches the expert difficulty. On the other hand, when answering a question incorrectly the difficulty of the next question goes down by one level for each incorrect answer until it reaches easy difficulty. After completing the game the player is met with the option to replay the game. When replaying the player has the option to enter their difficulty level. This means they start question 1 at their previously attained difficulty level, making it possible to get a higher final score.

4.2.3 Rewards. Before starting the game the player is informed there is a reward after completing the training with a minimum score of 200. After completing the game the player is rewarded with a certificate; which can be seen in Figure 4. This certificate is proof of completing the image steganography training. To ensure anonymity the name mentioned on the certificate can be entered before download, but is not stored.

Fig. 4. The certificate proving completion of the gamified training.

4.2.4 Feedback & Hypermedia. When the user answers a question wrong, an explanation about the question is given. From this explanation, they can understand why their answer was incorrect. When answering a question correctly they get a positive message and a link to some external media where the person could

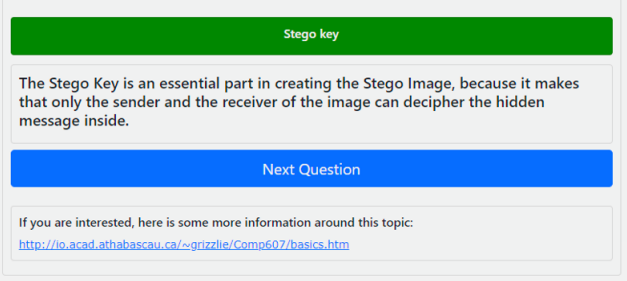

Fig. 5. Explanation and external links are given after an answer is given.

acquire additional information on the specific topic if they are interested. At the end of the game, a graph of their difficulty level throughout the game is shown as well as a list of topics, alongside links on these topics, which they could still improve upon. In Figure 5, an example is shown of feedback given by the game in the form of an explanation and a box indicating if the answer is correct or incorrect; in this case correct. Also hypermedia can be seen in the form of the link to external sources.

4.2.5 Time Limit. For completing the quiz a time limit of 10 minutes is set. This means that questions need to be answered, on average, in a minute. If a player has an average answering time above 1 minute, a message is displayed that states they need to hurry with answering the question to complete the quiz in time; an example of this can be seen in Figure 6. This message is to incentivize completing all ten questions in the allotted time.

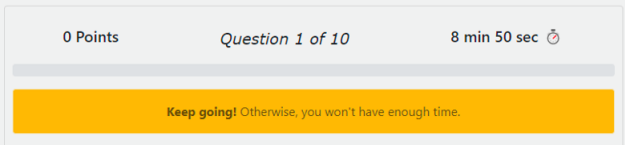

Fig. 6. Warning when time is running out.

4.3 Research Design

As mentioned before, the game is a web application. It is hosted on a website where people with the link can access the game. The game itself contains all relevant links to the consent form, and the pre-game and post-game surveys. Therefore, when distributing the game only the link to the game has to be shared.

Before playing the game, participants have to fill out a survey assessing their background knowledge and state of mind. The use of subjective reporting in research comes with the risk of introducing bias, introduces by the emotional state of the participant, into the survey data [4]. When looking at previously developed tools on the topic of cybersecurity, like the ones researched in chapter 2, this bias is not taken into account. To mitigate the risk of this bias we try to determine the emotional state of each participant, prior to testing the gamified training tool, by adding questions to the survey like: 'How are you feeling?', 'Are you experiencing any stress right now?', and 'Are you well-rested?'.

When participants are using the tool, game statistics are extracted to be analyzed. These results show what impact specific question categories or questions might have. For example, 'the multiple-choice questions are too easy' or 'question 3 is too hard, no-one was able to answer it right'.

For the post-game survey, the experience of the user is accessed. A Likert scale from 1 to 5 is applied to answer these questions, where 1 stands for strongly disagree, 2 stands for slightly disagree, 3 is neutral, 4 stands for slightly agree, and 5 stands for strongly agree. From this, the results are statistically evaluated by comparing them to a hypothetical value. For this purpose, we selected the one-sample one-tailed t-test and the one-sample Wilcoxon signed rank test [6, 42]. Even though the t-test is usually applied to continuous data, it is also applicable to small amounts of discrete data [2].

5 RESULTS

In this chapter, the results of the experimental study are shown. The results are reviewed and discussed in relation to the research questions. Possible other findings are also discussed.

5.1 Results

This section presents the results from both surveys and statistical data from the game. These results are qualitatively and quantitatively evaluated.

From the pre-game survey our population is analysed. 28% are female to 72% male. 67% are from the 'Universiteit Twente', 11% from the 'Universiteit van Amsterdam', and 22% from varies other universities in the netherlands. About 63% of participants are from an Information Technology background; this distribution can be seen in Figure 7. On average the participants rated their prior technical knowledge high and their cybersecurity awareness level average; as can be seen in Figure 8 and Figure 9 respectively. However, over 62% of participants indicated that they did not know what steganography was.

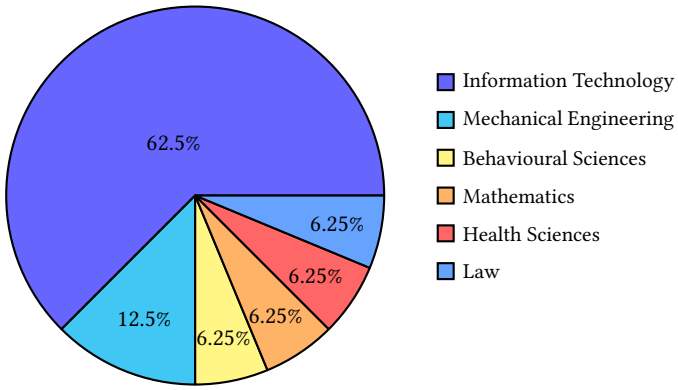

Fig. 7. Distribution of participants' studies.

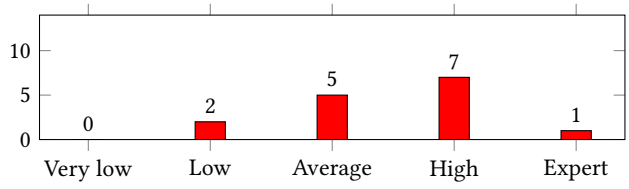

Fig. 8. Distrubution of technical knowledge.

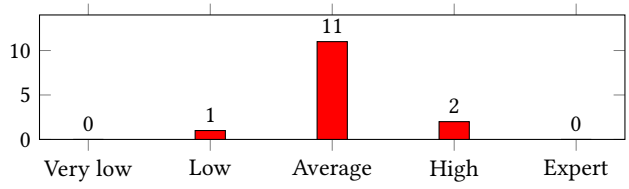

Fig. 9. Awareness of cybersecurity risks.

When looking at the game statistics we find an average score of 50 after a participant's first play-through. The average distribution is shown in Figure 10.

Fig. 10. Average amount of points among participants.

When looking at specific questions we find that most questions were very difficult, either due to unclear explanations or sheer difficulty; this is reflected in Figure 11. On average the participants had a score of 30% correct answers. There was no significant difference in groups based on gender, which university they were from, age, if they had prior training, or if they had prior steganography knowledge. We did find that the percentage of correct answers increased with their technical level; as can be seen in Figure 12.

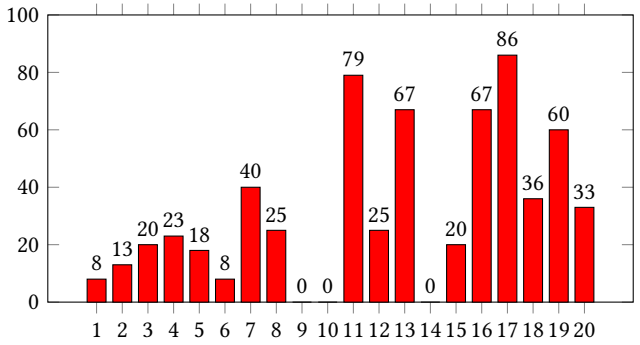

Fig. 11. Percentage a question was answered correctly.

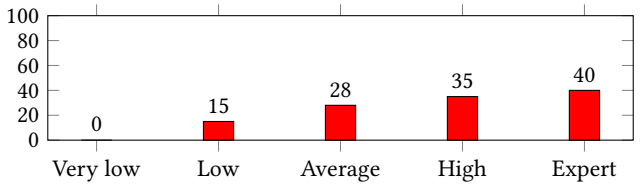

Fig. 12. Percentage of questions correct compared to participants' technical level.

The post-game survey contained some statements on properties of the tool, where participants gave a rating from 1 through 5 on how much they agree with the statement. From this data the mean value was deduced, where a rating of 3 or larger shows a positive effect on the specific property. Using this data we performed a one-sample one-tailed t-test, as well as a one-sample Wilcoxon signed rank test. The null hypothesis states that there is no significant possible effect on the property; a mean score of 3 or less. The critical value of the

t-test for 15 participants, power of 74%, a confidence level of 95%, and degrees of freedom of 14, is 1.761. For the Wilcoxon signed rank test, the critical value is 30. In Table 3 we find all the properties with their t and W values.

Table 3. Results for t-test and Wilcoxon test on different properties.

Property	t-value	passes t-test	W-value	passes Wilcoxon
Clear theory	1.434	✗	32.5	✗
Real-world link	8.281	✓	0	✓
Incr. knowledge (Cybersecurity)	3.795	✓	5	✓
Incr. knowledge (Steganography)	6.725	✓	0	✓
Engagement	0.851	✗	20	✓
Short Form	5.659	✓	3	✓

The statistical test show there is no significant proof of the clarity of the theory, and from the t-test only we do not find a significant improvement in engagement. However, from the Wilcoxon signed rank test we do find significance in improvement in engagement. Overall the participants enjoyed using the tool, which sparked interest in the cybersecurity topic of steganography, and from which they have acquired new knowledge.

5.2 Discussion

This section goes over the results from the study and relates them in terms of the research question in order to answer them.

To answer sub-research question 1, literature research was conducted. Here we identified previously developed gamification training tools on different cybersecurity topics. From these tools, effective gamification features were identified in stimulating engagement.

- Challenges
- Storytelling
- Rewards
- Time constraint
- Rich visuals
- A sense of control
- Hypermedia
- Scoreboards
- Personalization
- A clear structure
- Feedback

From this list, the most effective three features are identified, namely: *Challenges*, *Storytelling*, and *Rewards*.

In designing the training tool, the answer to sub-question 2 is consequently given. In the design, the following gamification features are represented.

- Challenges (by giving quiz questions and letting people figure out how to use different image steganography tools)
- Storytelling (by placing stories of real-world scenarios in the questions)
- Rewards (by giving points and a certificate which can be won)
- Time constraint (by setting a timer of 10 minutes)
- Hypermedia (by providing links to external sites for further investigation of the topics)
- Feedback (by showing an explanation to each question, and warning about time that has passed)

To answer sub-question 3, the survey results are used. Although an increase in engagement is not proven to be significant, we do find that players had high levels of enjoyment, sparked interest in the topic of steganography in the majority of participants, and 100% of participants indicated having acquired new knowledge using the training tool. This lack of engagement is mostly due to a lack of explanation and clarity making some of the questions very hard, or even impossible.

6 CONCLUSION

In this chapter the conclusions with respect to the research question are presented, as well as the limitations of the study, and possible next steps that can be taken to take this research to the next level.

Abundant literature is available on researching the most efficient application of steganography, as well as the application of gamification in the field of cybersecurity. However, image steganography training has not been put in a gamified context before. The novel gamified image steganography training tool is freely available for future research or public use. The game showed the potential in sparking interest in the topic in its participants and showed an effective learning experience. The main focus of this research was to evaluate the level of engagement with the training tool. Unfortunately in its current form, the engagement is not at the desired level.

6.1 Limitations

When doing research assumptions have been made from a more general space of gamification applied to cybersecurity. From this literature on gamified cybersecurity, effective techniques were identified. These techniques are assumed to be effective on the topic of steganography. To further prove this assumption more research should be done on the effect of gamification when applied to steganography training both in making content and improving the game features.

Also due to time constraints the study only involved a small sample size. To improve the power over the statistical model and improve the reliability of the research a bigger sample size should be followed in future research.

6.2 Future Work

When moving forward, the game should be expanded and improved with more interactive questions where people are able to play around with image steganography tools. Also, an improved user interface could greatly benefit the gaming experience and engagement level. Lastly, a better explanation of the topics within the tool is necessary as the topic of steganography is not general knowledge. When these features would be implemented, only then could be deduced if the tool is effective in aiding in image steganography training.

ACKNOWLEDGMENTS

I would like to thank Dr. D.K. Sarmah for her guidance as a supervisor during this project. Without her, this project would not have been possible. I would also like to thank Dr. S. Bayhan as well as S.S. Spuls for further guidance and advice during this period.

REFERENCES

[1] Program Ace. 2022. 2 types of gamification: Which one is right for you?: Programace. https://program-ace.com/blog/types-of-gamification/#:~:text=There%20are%202%20key%20approaches,âĂŞ%20structural%20and%20content-based.

[2] Admin. 2019. Can I use parametric analyses for my Likert scales? A brief reading guide to the evidence-based answer. https://lindeloev.net/can-i-use-parametric-analyses-for-my-likert-scales-a-brief-reading-guide/

[3] Ahmed Aleroud and Lina Zhou. 2017. Phishing environments, techniques, and countermeasures: A survey. *Computers Security* 68 (2017), 160–196. https://doi.org/10.1016/j.cose.2017.04.006

[4] Kine Askim and Stein Knardahl. 2021. The Influence of Affective State on Subjective-Report Measurements: Evidence From Experimental Manipulations of Mood. *Frontiers in Psychology* 12 (2021).

[5] Anupam Bairagi. 2023. ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security. (01 2023).

[6] Rebecca Bevans. 2022. Choosing the right statistical test: Types amp; examples. https://www.scribbr.com/statistics/statistical-tests/

[7] Arpit Bhayani. 2020. Everything that you need to know about image steganography. https://www.codementor.io/@arpitbhayani/internals-of-image-steganography-12qsxcxjsh

[8] Kristoffer Björklund. 2021. What's the Deal with Stegomalware? : The Techniques, Challenges, Defence and Landscape.

[9] Tom Cuchta, Brian Blackwood, Thomas R. Devine, Robert J. Niichel, Kristina M. Daniels, Caleb H. Lutjens, Sydney Maibach, and Ryan J. Stephenson. 2019. Human Risk Factors in Cybersecurity. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (Tacoma, WA, USA) *(SIGITE '19)*. Association for Computing Machinery, New York, NY, USA, 87–92. https://doi.org/10.1145/3349266.3351407

[10] Dictionary.com. 2022. *Cryptography.* Retrieved December 15, 2022 from https://www.dictionary.com/browse/cryptography#:~:text=noun,writing%2C%20as%20codes%20or%20ciphers.

[11] Designing Digitally. 2019. Structural gamification and content gamification: DDINC. https://www.designingdigitally.com/blog/structural-gamification-and-content-gamification

[12] Lauren S. Ferro, Andrea Marrella, Tiziana Catarci, Francesco Sapio, Adriano Parenti, and Matteo De Santis. 2022. AWATO: A Serious Game to Improve Cybersecurity Awareness. In *HCI in Games*, Xiaowen Fang (Ed.). Springer International Publishing, Cham, 508–529.

[13] Dr Zachary Fitz-Walter. 2021. What is gamification? education, Business amp; Marketing (2021 examples). https://www.gamify.com/what-is-gamification

[14] Vitaly Ford and Ambareen Siraj. 2020. GenCyberCoin: An Engaging, Customizable, and Gamified Web Platform for Cybersecurity Summer Camps and Classrooms. *J. Comput. Sci. Coll.* 35, 3 (jan 2020), 87–96.

[15] Hugo Gonzalez, Rafael Llamas-Contreras, and Francisco Ordaz. 2017. Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus. *Research in Computing Science* 146 (12 2017), 35–43. https://doi.org/10.13053/rcs-146-1-4

[16] itcho.io. 2023. *Download the latest Indie Games.* Retrieved January 22, 2023 from https://itch.io/

[17] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn)* 12 (02 2018), 150. https://doi.org/10.11591/edulearn.v12i1.7736

[18] Stylianos Karagiannis, Elpidoforos Maragkos-Belmpas, and Emmanouil Magkos. 2020. An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. In *Information Security Education. Information Security in Action*, Lynette Drevin, Suné Von Solms, and Marianthi Theocharidou (Eds.). Springer International Publishing, Cham, 61–77.

[19] Bally Kehal. 2023. *Steganography.* Retrieved January 21, 2023 from https://www.cybertraining365.com/cybertraining/Courses/Steganography

[20] Simon Kemp. 2022. *Digital 2022: Time spent using connected tech continues to rise.* Retrieved December 15, 2022 from https://datareportal.com/reports/digital-2022-time-spent-with-connected-tech

[21] Anastasia Khomych. 2022. App Gamification: 9 examples of mobile apps using gamification. https://blog.getsocial.im/is-gamification-the-only-way-for-apps-to-survive/#Gamification_in_e-learning_apps

[22] KidsAcademy.mobi. 2022. Gamification for Interactive Learning: Benefits amp; Ideas of interactive video quizzes to enhance student learning. https://www.kidsacademy.mobi/storytime/interactive-gamified-quizzes/#:~:text=Gamified%20quizzes%20can%20assist%20in,leading%20to%20better%20learning%20outcomes.&text=Besides%20motivating%20students%20to%20participate,competitive%20environment%20in%20the%20classroom.

[23] Tim Laning. 2022. Serious games, gamification and game-based learning: What's the difference? https://grendelgames.com/serious-games-gamification-and-game-based-learning-whats-the-difference/

[24] Bhanu Pratap Mahato. 2023. *Implement steganography techniques with different software's.* Retrieved January 21, 2023 from https://www.udemy.com/course/steganography/

[25] Fiona Fui-Hoon Nah, Qing Zeng, Venkata Rajasekhar Telaprolu, Abhishek Padmanabhuni Ayyappa, and Brenda Eschenbrenner. 2014. Gamification of Education: A Review of Literature. In *HCI in Business*, Fiona Fui-Hoon Nah (Ed.). Springer International Publishing, Cham, 401–409.

[26] CBS Statistics Netherlands. 2019. *1.2 million cybercrime victims.* Retrieved December 15, 2022 from https://www.cbs.nl/en-gb/news/2019/29/1-2-million-cybercrime-victims

[27] CBS Statistics Netherlands. 2020. *Less traditional crime, more cybercrime.* Retrieved December 15, 2022 from https://www.cbs.nl/en-gb/news/2020/10/less-traditional-crime-more-cybercrime

[28] CBS Statistics Netherlands. 2022. *Nearly 2.5 million people victims of cybercrime in 2021.* Retrieved December 15, 2022 from https://www.cbs.nl/en-gb/news/2022/09/nearly-2-5-million-people-victims-of-cybercrime-in-2021

[29] J. C. Nwokeji, R. Matovu, and B. Rawal. 2021. The use of gamification to teach cybersecurity awareness in information systems. In *Proceedings of the 2020 SIGED International Conference on Information Systems Education and Research*. 160–164. www.scopus.com

[30] NSA/NSF GenCyber Program. 2023. *Inspiring the next generation of cyber stars.* Retrieved January 18, 2023 from https://www.gen-cyber.com/

[31] Qualtrics. 2022. Qualtrics XM // the leading experience management software. https://www.qualtrics.com/uk/?rid=ip&prevsite=en&newsite=uk&geo=NL&geomatch=uk

[32] UT Research GDPR Registration. 2022. UT Research GDPR Registration. (November 2022). https://www.utwente.nl/en/bms/datalab/research-data-and-gdpr/research-registration/.

[33] Michael Sailer, Jan Ulrich Hense, Sarah Katharina Mayr, and Heinz Mandl. 2017. How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. *Computers in Human Behavior* 69 (2017), 371–380. https://doi.org/10.1016/j.chb.2016.12.033

[34] Zia A. Sardar. 2020. *Cryptography: How it Helps in our Digital World.* Retrieved December 15, 2022 from https://www.mouser.com/pdfDocs/Maxim_AN7253.pdf

[35] Ethics Committee Computer Information Science. 2022. Ethics committee: faculty of electrical engineering, mathematics and computer science (eemcs). (November 2022). https://www.utwente.nl/en/eemcs/research/ethics/.

[36] Mukta Sharma. 2015. Steganography is the art of Hiding Data. *IJARSE* 4 (03 2015).

[37] Bharat Sinha. 2015. Comparison of PNG amp; JPEG format for LSB Steganography - IJSR. https://www.ijsr.net/archive/v4i4/29031501.pdf

[38] B. K. Sinha. 1970. [PDF] comparison of PNG amp; JPEG format for LSB steganography: Semantic scholar. https://www.semanticscholar.org/paper/Comparison-of-PNG-%26-JPEG-Format-for-LSB-Sinha/321f900c6592325fcaf74689c92221935e8f7a98

[39] LexisNexis Risk Solutions. 2022. LexisNexis Risk Solutions biannual CybercrimeReport. Technical Report. LexisNexis Risk Solutions.

[40] Franklin Tchakounte, Leonel Wabo, and Marcellin Atemkeng. 2020. A Review of Gamification Applied to Phishing. https://doi.org/10.20944/preprints202003.0139.v1

[41] Kaspersky ICS CERT | Kaspersky Industrial Control Systems Cyber Emergency Response Team. 2022. Steganography in attacks on industrial enterprises (updated): Kaspersky ICS CERT. https://ics-cert.kaspersky.com/publications/reports/2020/06/17/steganography-in-attacks-on-industrial-enterprises/

[42] nQuery Team. 2022. What statistical test should I use? https://blog.statsols.com/types-of-statistical-tests

[43] Sansec Team. 2020. Payment skimmer hides in social media buttons. https://sansec.io/research/svg-malware

[44] K. Thangadurai and S. Devi. 1970. [PDF] evaluation of LSB based image steganography technique for various file formats: Semantic scholar. https://www.semanticscholar.org/paper/Evaluation-of-LSB-Based-Image-Steganography-for-Thangadurai-Devi/584a8f802e89d847558d1ea2d5a85931c9fd9dc0

[45] Ankur Trapasiya. 2012. PNG file size increase in LSB Steganography. https://stackoverflow.com/questions/13660501/png-file-size-increase-in-lsb-steganography

[46] Market Trends. 2021. Today's Digital World and key cryptography. https://www.analyticsinsight.net/todays-digital-world-and-key-cryptography/#:~:text=Cryptography%20protects%20information%20by%20transforming,the%20code%20used%20for%20protection!

[47] Ministerie van Justitie en Veiligheid. 2016. Forms of cybercrime. https://www.government.nl/topics/cybercrime/forms-of-cybercrime#:~:text=Common%20forms%20of%20cybercrime%20include,personal%20information%20(identity%20theft)%3B

[48] Wikipedia. 2022. Capture the flag (cybersecurity). https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity)

[49] Wikipedia. 2023. *Serious game*. Retrieved January 21, 2023 from https://en.wikipedia.org/wiki/Serious_game
[50] Wikipedia. 2023. *Steganography*. Retrieved January 21, 2023 from https://en.wikipedia.org/wiki/Steganography
[51] Tania Williams and Omar El-Gayar. 2022. Design of a Virtual Cybersecurity Escape Room. In *National Cyber Summit (NCS) Research Track 2021*, Kim-Kwang Raymond Choo, Tommy Morris, Gilbert Peterson, and Eric Imsand (Eds.). Springer International Publishing, Cham, 60–73.
[52] Simon Wiseman. 2017. Stegware – Using Steganography for Malicious Purposes. https://doi.org/10.13140/RG.2.2.15283.53289