Design and Validation of Serious Game on Steganography for Higher Education

FEMKE WEIJSENFELD, University of Twente, The Netherlands

Serious games are increasingly employed in educational environments to enhance student engagement and improve learning outcomes. Research indicates that these games positively impact holistic understanding and long-term knowledge retention. Steganography, the practice of concealing information in plain sight to prevent detection, is a critical topic in cybersecurity. Despite its importance, teaching steganography often relies on traditional methods such as lecturing and reading books, partly due to the limited availability of engaging serious games tailored to this subject. This study aims to design and evaluate an interactive, narrative-based serious game focused on steganography in order to help teachers enhance their lessons in an engaging way. To assess the game's effectiveness, two groups of in total 54 participants in higher education in the Netherlands have participated in its validation: one group has played the designed game, while the other group has studied the same content through a textual resource. Both groups then provided feedback on their engagement levels in the User Engagement Scale Short Form and completed a knowledge test. The study has analysed this data and found that there is a significant difference experienced in engagement between the groups. No significance difference between the scores on the knowledge test was found. The results from this research could establish the game as a valuable teaching tool, enriching university curricula and enhancing students' learning experiences in cybersecurity education.

CCS Concepts: • **Social and professional topics** → **Computer science education**; • **Security and privacy**;

Additional Key Words and Phrases: Steganography, Cybersecurity Education, Serious Games, Narrative-based Learning

1 INTRODUCTION

Steganography is the practice of concealing information within another object in such a way that a potential eavesdropper remains unaware of its presence. A non-digital example is writing a visible letter while embedding an invisible message between the lines using lemon juice, which is a common science experiment[1]. An interceptor would see only the visible text, oblivious to the hidden content. Similarly, in the digital realm, steganography involves altering data—such as pixels in an image or bits in a file—minimally to encode a hidden message. For instance, slight adjustments to pixels can allow one to conceal information without obvious visual cues. This technique enables covert communication, historically used by spies and, alarmingly, by malicious actors. It has been reported that the 9/11 attacks were planned using steganography to share covert messages among terrorists [10].

Steganography poses not only a communication threat, but also a cybersecurity risk. Malicious software can be embedded in data objects such as images or PDF files, downloaded unknowingly by users [11]. These risks underline the importance of educating students about steganography—what it is, its potential dangers, how it works, and strategies for mitigating its risks.

Steganography has emerged as a significant concept within the field of cybersecurity, gaining increasing attention in cybersecurity education across various institutions [14]. However, the teaching methods for introducing such concepts vary widely. Traditional approaches include lectures, videos, or other teacher-provided materials [23, 26]. While effective, these methods may lack engaging factors necessary to optimize learning outcomes.

Engagement is critical in education, as it enhances students' learning experiences and outcomes [9, 20, 33]. Since serious games are designed to raise engagement, they allow students to enjoy the learning process while improving retention and understanding. This principle may also apply to teaching steganography. An engaging serious game on this topic could improve both engagement and learning outcomes.

Although numerous serious games for educational purposes exist, such as *DimensionM*, *Re-Mission*, and *Cyber Awareness* [13, 15, 40], to the best of our knowledge, no engaging serious game specifically designed for teaching steganography is currently available. Furthermore, the level of engagement provided by existing serious games varies significantly across different implementations [13].

Due to the absence of an engaging serious game on steganography [35], educators often rely on traditional teaching methods. This lack of engaging tools may negatively impact students' learning experiences and hinder their understanding of the subject.

This research aims to address this gap by designing an engaging serious game on steganography and testing its impact on test scores and self-reported engagement. Validation of the game revealed no significant difference in test scores when compared to a group of students who learned the material through reading a text. However, the game demonstrated higher levels of engagement compared to the traditional text-based approach.

By providing this tool, we think that educators now have access to a resource that enhances lesson delivery, improves student engagement, and fosters learning outcomes in the domain of steganography.

2 RESEARCH GOAL & REQUIREMENTS

The objective of this research is to design and develop a serious game that gives teachers an interactive and engaging tool for teaching university students the concept of steganography effectively. This research is guided by the following research goal (RG):

RG: Design and implement an engaging serious game to teach students about steganography.

To satisfy the research goal (**RG**), the requirements of the game must be clear. As the research goal suggests, the first requirement **RQM1** is: The game must be more engaging than the traditional teaching method of reading a text about the topic.

[1] See KiwiCo, SteveSpangler, Little House of Science.com and British Science Week

TScIT 42, January 31, 2025, Enschede, The Netherlands

In addition to being engaging, the game is designed to provide students with an introduction to the fundamentals of steganography. To this end, specific learning goals have been established, focusing on equipping students with foundational knowledge of steganography. To inform the development of these learning goals, the article An Overview of Steganography by Kessler (2011) [19] was reviewed for inspiration. Furthermore, various online resources[2] and academic papers [36, 39] were analysed to better understand the key concepts and teaching approaches related to steganography. Based on these sources, the following learning goals were developed:

Learning Goals

Steganography & Cryptography:

(1) The student is able to classify example situations of either cryptography, steganography or a combination of both.
(2) The student is able to formulate an example in which the usage of steganography is preferred over cryptography.

Image Steganography:

(3) The student is able to adjust pixels in an image to embed a hidden message.
(4) The student can determine which image from a given selection of equally sized images could be best used for steganographic purposes.
(5) The student can give an example of a context in which steganography can be used for sharing secret messages.

The Big Picture:

(6) The student can give an example of a context in which steganography is used for embedding malicious software.
(7) The student can identify similarities between image steganography and audio steganography.
(8) The student can recite the method of embedding a hidden message into a medium.
(9) The student knows that a stego key is necessary to uncover the message in complex algorithms.

StegWare & StegAnalysis:

(10) The student is able to explain why attackers may use steganography within their malicious software as opposed to not using steganography.
(11) The student is able to put a pseudocode in the right order for an attack with Stegware.

This consideration leads to the second requirement, **RQM2**: Following the completion of the game, students must demonstrate knowledge on a test covering the defined learning goals that is at least equivalent to the performance of students who acquire the same knowledge by reading a text about steganography.

The final requirement, **RQM3**, specifies that the game must be accessible via a web browser. This criterion is critical for a wide range of educational contexts, as web browsers are universally available across most operating systems. Furthermore, it eliminates the need for students or IT staff to download and install additional software, thereby enhancing accessibility and convenience.

[2]The following websites were consulted for additional insights: Codementor, EC-Council, and TechTarget.

3 RELATED WORK

Serious games have been shown to enhance holistic understanding and support long-term retention of knowledge [8]. Additionally, students who participate in serious games often report higher self-perceived learning outcomes compared to those in traditional classroom settings [33]. Consequently, serious games are regarded as highly effective educational tools. This section examines existing serious games to assess their alignment with the defined research requirements.

To the best of our knowledge, the only serious game addressing the topic of steganography was *StegAware*, developed by Simon [35]. However, the game did not elicit significant self-reported engagement—a critical factor in the success of serious games, as engagement is a key driver of their effectiveness [31]. Simon identified several areas for improvement, including the need to enhance the game's aesthetic appeal, incorporate tools for hands-on image steganography, and provide clearer explanations of the concept. Consequently, this serious game does not satisfy **RQM1**, which emphasizes the importance of engagement.

While sufficiently engaging serious games explicitly focused on steganography are not currently available, numerous educational serious games have been successfully developed in various other domains, demonstrating their effectiveness in enhancing learning outcomes [40]. For instance, *Virtual Age* is a serious game designed to teach students about evolution [7, 8]. The game employs attractive graphics, autonomy, clear goals, and competitive elements to foster immersion [8]. Players must occupy resource areas to reproduce more offspring or summon new species. However, as it was developed in Adobe Flash CS5, it is no longer accessible.

Another notable example is *DimensionM*, a game that integrates mathematics questions into its sci-fi storyline. Research indicates that the game positively impacts student achievement in public high school settings [18]. DimensionU[3] has expanded on this concept with additional games, such as *TowerStorm*, *Meltdown*, and *Velocity*, where students are rewarded for correctly answering questions. However, these games are not freely available.

Re-Mission[4] is another example of a serious game, aimed at educating cancer patients about the disease and its treatment. In this shooter game, players combat cancer cells and manage side effects. Studies have shown that *Re-Mission* can be an effective tool for health education [4].

The aforementioned games, while successful in their respective fields, do not pertain to computer science or cybersecurity. Within the cybersecurity domain, examples of educational serious games include *Cyber Awareness*[5] and *Cyber Mission*[6]. These freely available games involve players investigating cases, making decisions, and answering questions to progress through the game. They have demonstrated exemplary effectiveness in terms of design, delivery, and game-based learning outcomes [15]. However, steganography is not a central theme in these games.

Consequently, the games discussed are unlikely to meet **RQM2**, as their primary focus does not align with the topic of steganography.

[3]https://www.dimensionu.com/
[4]https://hopelab.org/history/
[5]https://public.cyber.mil/training/cyber-awareness-challenge/
[6]https://www.cybermission.tech/

4 GAME DESIGN

With the requirements established, the game must be designed to ensure that each requirement is met. The following sections will detail how the requirements outlined in Section 2 are addressed.

4.1 RQM1: Engagement

Narrative storytelling has been shown to enhance engagement, immersion, and learning outcomes in serious games [25]. Its effectiveness is not just limited to gaming, it has also been shown to be effective in adult education [5].

Therefore, the new game was designed as a narrative-driven serious game, with the story serving as its central focus. Players will navigate a fictional scenario involving hidden messages and digital clues, making choices to progress through the narrative. During this journey, small puzzles are integrated to reinforce learning objectives [6]. These puzzles include tasks such as identifying steganographic methods in images and decoding messages by analysing pixel values. This interactive design ensures that participants not only learn theoretical concepts, but also practice applying them in simulated scenarios.

Due to incorporation of interactive and engaging game design strategies, such as decision-making and narrative elements, which are known to enhance students' engagement [5, 25, 33, 40], we expect to meet **RQM1**.

4.2 RQM2: Steganography Learning Goals

To meet **RQM2**, a story has been developed that incorporates the learning goals outlined in Section 2. The story begins with a problem related to cryptography, accompanied by an explanation for students unfamiliar with the topic. Following this, the student investigates a room to collect evidence. During the investigation, the student encounters image steganography, which is further explained and analyzed at the protagonist's headquarters. Finally, the student transitions to the computer world, taking on the role of StegWare to infiltrate the enemy's system. This task is designed to be challenging, with the student's choices directly influencing the outcome of the story.

Figure 1 illustrates the story as a directed graph, where each node represents a character speaking a sentence and possibly offering choices. As shown, players can take various paths, personalizing their adventure. A full interactive view and more details about each story node are available at https://stegadventure.femkew.nl/story. Appendix A outlines how these nodes connect to the learning goals.

Additionally, to meet **RQM2**, elaborative feedback is integrated within the game, as it increases higher order learning outcomes [37]. The feedback given is not exaggerated as that may work in a negative way instead [2, p. 145].

Finally, jokes were integrated into the game, as humour has been shown to enhance student performance [34].

4.3 RQM3: Web browser

The game is developed using HTML, CSS, and JavaScript to ensure it can be hosted on a web server and accessed by users across different operating systems without requiring downloads. This approach increases availability for participants. The Vue.js framework has been employed for the front-end due to its component-based architecture, which facilitates maintainability and scalability. Implemented front-end examples can be seen in Figure 2 and Figure 3.

On the back-end, the game uses Laravel, a PHP framework, to handle tasks such as saving participant data to a database. Laravel is chosen for its built-in security and database management features, making it ideal for handling research data.

After the implementation phase, the game was tested by two individuals to ensure stability and prevent bugs. The game can be found played at stegadventure.femkew.nl/game and the source code can be found at https://github.com/fkmke/stegadventure.

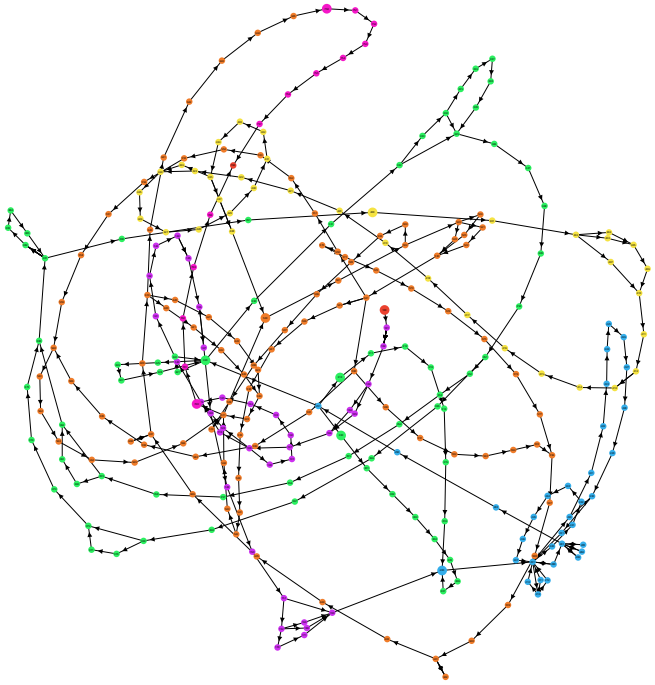

Fig. 1. The game story, represented as a directed graph, shows the different paths players can take in the story (zoom option at https://stegadventure.femkew.nl/story)

Fig. 2. Screenshot of game showing an interaction with another character

Fig. 3. Screenshot of game showing options for the player to choose what to investigate

5 METHODOLOGY OF VERIFICATION

Verification is necessary to determine whether the newly developed game meets the requirements and achieves the research goal. **RQM3** is satisfied, as the game is hosted on a website. However, to assess whether **RQM1** and **RQM2** are met, human participants are required.

The game will be evaluated against the traditional teaching method of reading a text [23, p. 2]. Group A will learn through playing the game, while Group B will learn by reading a text on steganography. This setup allows for a comparison between the two learning methods with regards to engagement and learning.

5.1 Testing RQM1: Engagement

To measure engagement, participants will complete the User Engagement Scale Short Form (UES-SF) to assess their perceived engagement with the game or the text [30]. The short form was selected for its reliability and time efficiency, minimizing participant burden.

The UES-SF questions were slightly adapted to align with the experiment's context and literacy level, as recommended [12]. The modified questions and changes are detailed in Appendix B.

The results from the User Engagement Scale Short Form (UES-SF) have been analysed following the guidelines of the original author [30]. Engagement scores will be compared between Group A and Group B using independent-samples t-tests, provided the data is normally distributed. The t-test checks whether there is a significant difference between the two groups. If the data is not normally distributed, the Mann-Whitney U test will be used, as it is suitable for non-normally distributed data. Normality will be assessed using the Shapiro-Wilk test. The null hypothesis for the t-test is that there is no significant difference in engagement between the two groups.

5.2 Testing RQM2: Steganography Learning Goals

To measure whether the learning goals are met, participants will perform a test to test their knowledge. This test will include questions based on the Revised Bloom's Taxonomy [1], covering cognitive levels such as Remember, Understand, and Apply. For example:

- A 'Remember' question may ask participants to recall the definition of StegWare.
- An 'Apply' question may involve adjusting pixel values in an image to encode a message.

This structured approach ensures that understanding is assessed across different cognitive levels.

The knowledge test yields a score on a scale from 1 to 10 and consists of 9 multiple-choice questions, each worth 6 points for a completely correct answer. To discourage guessing, points are deducted for incorrect answers, and an "I don't know" option is included, as described in Method 13 by Kanzow et al. (2023) [17]. Without this, the test score data could be skewed. The "I don't know" option enhances test reliability [24, 32], though it introduces more bias than traditional right-answer scoring [24, 32]. For this research, reliability is prioritized over minimizing bias.

The scoring formula is as follows:

$$\frac{\max(\text{obtained points}, 0)}{\text{total points available}} \times 9 + 1$$

This formula ensures that scores range from 1 to 10. The final scores of Group A and Group B will be compared using an independent-samples t-test to assess any significant difference between the groups. If the data is not normally distributed, the non-parametric Mann-Whitney U test will be applied.

The knowledge test is peer reviewed by five people, of which three have a teaching background, ensuring clarity and validity.

5.3 Time Analysis

The time participants spend reading the text or playing the game is measured. Correlations between the time spent and the knowledge test score will be examined to assess learning effectiveness.

5.4 The process

The participants primarily consist of university students in the Netherlands, aged 17 to 30, as they represent the target audience for the game. Participants will be randomly assigned to two groups: Group A (playing the game) and Group B (reading a text), ensuring minimized selection bias.

The process that participants in both groups undergo is illustrated in Figure 4, and will be described below in detail.

Both Group A and Group B will begin by completing the consent form. Group A will then play the serious game on steganography, designed to take approximately 20 minutes. Group B will read a text on the same concepts, supplemented with visuals for clarity, also taking about 20 minutes. Afterward, participants will complete the UES-SF. Following the engagement survey, participants proceeded to take the same knowledge test.

At the end of the experiment, both groups are asked for feedback on the text they read or the game they played, or anything else that participants want to share, ensuring qualitative insights in the participants' thoughts.

If a participant fails to complete the knowledge test or the UES-SF, they have been excluded from the analysis.

All data collection (game decisions, surveys, and knowledge tests) will take place on a single online platform, which reduces participant

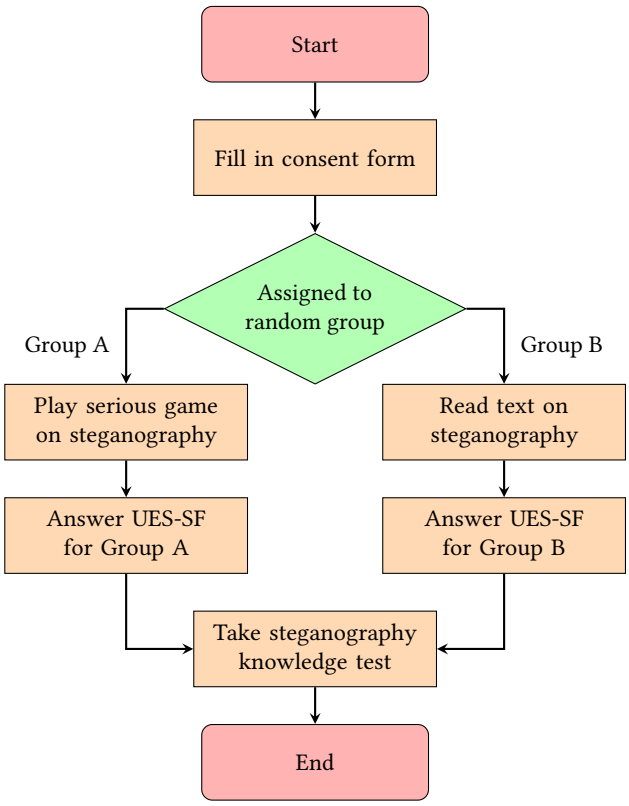

Fig. 4. The process that participants in this study will follow

burden and ensures ease of access. This approach eliminates the need for participants to navigate between multiple systems.

The whole process has been implemented as an web application which can be found at https://github.com/fkmke/stegadventure. How to adjust and analyse the game can be found in the readme.

5.5 Minimum Number of Participants

To determine the minimum required sample size before participants are recruited, we conducted a power analysis [16], focusing on the means of the knowledge test scores. We assumed an expected standard deviation of 1.5 points based on prior teaching experience. A statistical power of 0.8 and a significance level of 0.05 were chosen. The analysis tested three potential population mean differences: 1 point, 1.5 point and 2 points. The results of the power analysis are summarized in Table 1.

The preferred mean difference between the test scores is 1 point, which would reflect a substantial difference in test scores between the two groups. However, this would require a minimum of 74 participants, which may not be feasible within the scope of the current study. Therefore, this study will target a mean difference of 1.5 points between the groups, which would still allow us to detect a significant effect with a minimum of 34 participants, which is feasible as well within the scope of this research project.

Table 1. Power analysis for two-sided test assuming noncentral t-distribution and equal group variances, where $|\mu_A - \mu_B|$ is the mean difference between the test scores of Group A and B

Test Assumptions	$\lvert\mu_A - \mu_B\rvert = 2$	$\lvert\mu_A - \mu_B\rvert = 1.5$	$\lvert\mu_A - \mu_B\rvert = 1$
N1	10	17	37
N2	10	17	37
Actual Power	0.805	0.807	0.808
Power	0.8	0.8	0.8
Std. Dev	1.5	1.5	1.5
Effect Size	1.333	1.000	0.667
Sig.	0.05	0.05	0.05

To ensure adequate statistical power, we plan to recruit additional participants beyond the minimum required, accounting for potential dropout or incomplete data.

6 THREAT TO VALIDITY

A primary threat is participant selection. Although participants are randomly assigned to groups, certain characteristics may disproportionately appear in one group, particularly with fewer participants. To mitigate this, participant characteristics that could influence the experiment will be carefully analysed to assess their potential impact.

Another threat is the User Engagement Scale, as it measures only components of engagement rather than all aspects [27]. However, the scale is widely used, and expected effects have been observed in previous studies [28–30]. Thus, it is considered reliable enough to assess engagement differences in this study.

7 RESULTS & DISCUSSION

A total of 54 participants took part in the study, equally divided between Group A and Group B. First, the participants' characteristics, such as education level and prior knowledge, are examined to ensure they are equally distributed across groups. Next, knowledge test scores and study time are discussed, followed by an analysis of the User Engagement Scale scores. Finally, the responses to the open-ended questions are reviewed. A significance threshold of 0.05 is used for all statistical analyses.

7.1 Participant Characteristics

Participants were randomly assigned to groups. To check for any unintentional skew, statistical analysis was performed, with results shown in Table 2. For ordered multiple-choice questions (e.g., 'Very Low', 'Low', etc.), the Mann-Whitney U Test was used, mapping values from 'Very Low' = 1 to 'Expert' = 5. The ages of both groups were also analysed using the Mann-Whitney U Test, as the age distribution was not normal. A Chi-Square Test was conducted for Main Expertise, as the categories are independent; however, some expected frequencies were below 5, which may affect the validity of the test due to insufficient respondents in certain expertise categories.

Table 2. Table showing whether statistical differences have been found between the characteristics of the two groups

Characteristic	Test	Statistic	p-value	Difference
Age	Mann-Whitney U	$U = 391.5$	0.6437	no
Education	Mann-Whitney U	$U = 360.5$	0.9218	no
Main Expertise	Chi-Square Test	$X^2 = 4.23$	0.2380	no
Gaming Experience	Mann-Whitney U	$U = 295.0$	0.1783	no
Steganography Pre-knowledge	Mann-Whitney U	$U = 312.0$	0.3416	no
Cybersecurity Pre-knowledge	Mann-Whitney U	$U = 204.0$	0.0031	**yes**

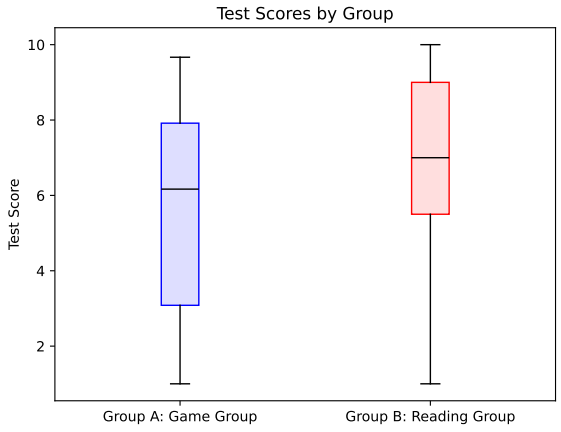

Fig. 5. Knowledge test scores box plot by group

The statistical tests show that there is a statistical difference in the cybersecurity pre-knowledge between the groups. Group B, the reading group, has a statistically higher significant number of participants with better cybersecurity pre-knowledge than Group A. The other possible characteristics that may influence test score seem to be evenly distributed amongst the groups, minimising those influencing factors.

Spearman's Rank Correlation Coefficient was calculated to assess whether higher cybersecurity pre-knowledge correlates with higher test scores. The coefficient of 0.4458 indicates a medium positive correlation [21, p. 213]. Furthermore, the p-value of 0.0007 confirms that this correlation is statistically significant.

Since the reading group has higher cybersecurity pre-knowledge, and higher pre-knowledge is associated with better test scores, caution is needed when interpreting the test scores.

7.2 Test Scores

The knowledge test scores are shown in the box plot in Figure 5. According to the Shapiro-Wilk Test (Table 3), the scores for both groups are likely normally distributed, as the p-values for both Group A and Group B exceed the 0.05 threshold for statistical significance. Therefore, a t-test was performed. Although the mean and median scores were lower for Group A, no significant difference was found between the groups. This is reflected in the p-value from the t-test (Table 3), which is greater than 0.05, meaning we fail to reject the null hypothesis that there is no difference in the means. This is likely because the minimum and maximum test scores are similar across both groups, with no outliers. Thus, **RQM2** has been met, as students using the game as a learning method performed equally to those reading the text.

The power of the t-test is 0.3045, with a Cohen's d of -0.4014. This indicates that the conclusion of "no significant difference" is not robust, as the test lacked sufficient sensitivity to reliably detect a difference. With only about a 30% chance of detecting a true effect, the test's power could be improved by revisiting either the test design or increasing the sample size.

One potential improvement in test design could be to focus on a single main expertise group, as a statistically significant difference was found in the means of the test scores from the main expertise groups according to the Kruskal-Wallis H Test ($H = 12.4985$, p-value = 0.0058). The Kruskal-Wallis Test was used instead of the ANOVA, as the 'Professions and applied sciences' group was not normally distributed, according to the Shapiro-Wilk Test.

This new test design was applied to the current data, focusing on the 'Formal Sciences' expertise group, as it had the most data points (Group A: 13, Group B: 16). Since the data for both groups was normally distributed (Group A: p-value = 0.8030, Group B: p-value = 0.2251), a t-test was applied, which again showed no significant difference between the test scores ($t = -1.8926$, p-value = 0.0692). However, the power increased to 45% (with a Cohen's d of -0.7066), despite having 25 fewer participants compared to the previous analysis. This suggests that focusing on participants from the same field can increase power, though increasing the sample size is still necessary.

The power could not be analysed for the other main expertise fields, as 'Professions and applied sciences' was not normally distributed, and 'Humanities and social sciences' and 'Natural sciences' had too few data points to assess normality. Therefore, it is not possible to determine if this trend holds for other expertise fields with the current sample size.

7.3 Time Analysis

The time that participants took to read the text or play the game has been measured and are shown in Figure 6. According to the Shapiro-Wilk Test, both groups are likely normally distributed and therefore a t-test is performed which results in $t = 7.0524$ and p-value = $4.0824 \cdot 10^{-9}$. Cohen's d is 1.9194 which means that there is a 97.3% chance that a participant from Group A, the game group, takes longer than the mean of the study time from Group A [22]. The power of the test, rounded to four decimals, is 1.0000, meaning that there is almost a 100% chance of detecting a true effect. The

Table 3. Statistical analysis of the knowledge test scores

Shapiro-Wilk Test Results		
Group	A	B
W	0.9269	0.9295
p-value	0.0581	0.0671
T-Test Results		
T-Statistic	-1.4472	
p-value	0.1539	
conclusion	no significant difference	

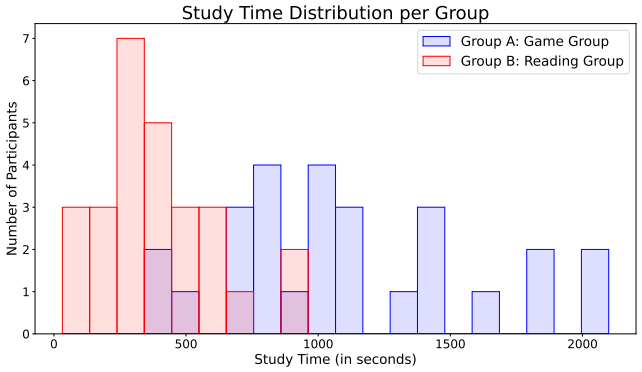

Fig. 6. Histogram showing time used to study per group (note: the mixed colour is overlap)

game groups takes a significantly longer time to complete the game than the reading group takes to read the text.

If we assume that no significant effect between the test scores of the two groups is a true effect (Section 7.2), then we can say that Group B, the reading group, has a higher learning efficiency, since they have a shorter study time for the same learning outcome.

7.4 User Engagement

The User Engagements Scale (UES) scores given by the participants are plotted in Figure 7. The scores from both groups are likely normally distributed according to the Shapiro-Wilk Test and therefore a t-test is applied (see Table 4). Since Group B contains one outlier, and the t-test is sensitive to outliers [3], the statistical tests are also applied without the outlier. However, both with and without the outlier, the null hypothesis, there is no difference in the means of the UES scores, is rejected, since the p-values of the t-tests are lower than 0.05. This means that there is a significant difference in the UES scores: Group A experiences a higher engagement according to the UES-SF.

The power of the UES test is 0.7061 (with a calculated Cohen's d of 0.6938), which means there is approximately a 71% chance of detecting a true effect. Therefore, we can say with relative confidence that there is an effect of difference in engagement between the two groups. Since playing the game is highly likely more engaging than reading a text, it can be said that **RQM1** has been met.

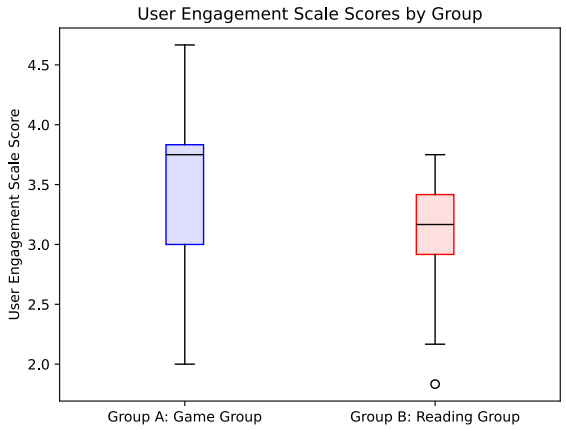

Fig. 7. User Engagement Scale Short From (UES-SF) scores box plot by group

Table 4. Statistical analysis User Engagement Scores

With outlier			Without outlier		
Shapiro-Wilk Test Results			**Shapiro-Wilk Test Results**		
Group	A	B	**Group**	A	B
W	0.9321	0.9343	**W**	0.9321	0.9625
p-value	0.0779	0.0882	**p-value**	0.0779	0.4433
T-Test Results			**T-Test Results**		
T-Statistic	2.5493		**T-Statistic**	2.3308	
p-value	0.0142		**p-value**	0.0246	
conclusion	significant difference		**conclusion**	significant difference	

7.5 Open participant responses

After the experiment, participants had an option to leave a comment. The exact questions that were asked were as follows: "Do you have any improvements for the game?" or "Do you have any improvements for the text you read?" and "Anything else that you would like to share?". Therefore, it should be noted that the amount of positive comments could be less, since the given questions asked for improvements, and not explicitly what the participant likes.

The participants' comments were categorised to facilitate a clearer understanding of their responses and the frequency of recurring themes. These categorised comments are detailed in Appendix C.

7.5.1 Comments about the game. Regarding the game's aesthetics and overall experience, participants appreciated the game but noted that its visuals appeared amateurish. Several participants suggested adding sound effects to enhance the immersive experience. Additionally, they requested clearer or more detailed explanations on key topics, such as the distinction between cryptography and steganography, selecting appropriate images for steganography, and locating messages within the Least Significant Bits (LSB) of an image.

Participants enjoyed the humorous elements and witty responses in the game but felt that the amount of information presented was overwhelming and cluttered at times. Overall, however, the game was positively received and described as "fun" or "good."

7.5.2 Comments about the steganography text. Participants who read the text primarily requested clearer explanations on locating messages within the Least Significant Bits (LSB) and understanding the concept of StegWare. One participant mentioned that the explanation of the stego key was boring. Several participants suggested including more real-life examples to enhance comprehension.

Some grammar mistakes in the text were noted and described as distracting. Additionally, one participant remarked that certain information about steganography, such as references to images containing scripts, appeared outdated. Despite these issues, the text was generally well-received and described as "a good read."

7.6 Comparison with StegAware

As presented in Section 3, to our knowledge, only one other serious game on the topic of steganography has been developed, namely StegAware by Simon [35]. A detailed comparison of the two studies is provided in Appendix D. The methodologies and power analyses reveal significant differences in approach and reliability of findings. StegAdventure employs established scales and peer-reviewed tests, ensuring a more objective evaluation of learning outcomes and engagement. In contrast, StegAware relies on self-reported measures and a smaller sample size, which limits the robustness of its conclusions. Consequently, determining which game achieves higher learning outcomes remains challenging.

8 FINAL CONSIDERATIONS

The game was designed and implemented in a web browser to test whether this new architecture meets the set requirements. Since the game is playable in a web browser, **RQM3** has been fulfilled.

To assess whether **RQM1** and **RQM2** have been met, an experiment with human participants was conducted. A total of 54 participants were involved in the game validation, equally divided into Group A (game group) and Group B (reading group). Although participants were randomly assigned, individuals with higher cybersecurity pre-knowledge were predominantly placed in Group B, which introduced a potential bias, as those with higher pre-knowledge scored better on the knowledge test.

There appears to be no significant difference in the knowledge test scores between the learning methods of Group A and Group B, which satisfies **RQM2**. However, the power of the test was only 30%, suggesting a low likelihood that the observed effect is reliable. The test's power could potentially be increased by focusing on participants with the same main expertise.

Moreover, the study time before the knowledge test was taken is significantly lower for Group B. If we assume that it is true that there is no significant difference between the knowledge test scores, then this suggests that Group B had better learning efficiency, as they achieved the same results with less study time.

However, despite Group B's higher learning efficiency, Group A reported significantly higher engagement, according to the User Engagement Scale, which satisfies **RQM1**. Ultimately, teachers can decide whether engagement or study efficiency is more important when determining whether to use the game in class.

To conclude, all requirements seem to be met and therefore the research goal **RG** has been reached. Thus an engaging serious game to teach students about steganography has been created.

For future work, several avenues can be explored. One limitation of this game validation methodology is that knowledge retention was not tested. A follow-up knowledge test could be conducted at a later stage to assess whether the game leads to higher knowledge retention than reading the text, due to its higher engagement [8].

Additionally, a study following the same methodology as presented in this paper could focus on a single main expertise (e.g., computer scientists or nurses) with a larger participant pool. This would likely increase the power of the knowledge test comparison. Alternatively, a new validation methodology could be developed to further enhance the power of the knowledge test comparison.

9 RECOMMENDATIONS

Teachers can use the developed game in class as an engaging introduction to steganography by visiting https://stegadventure.femkew.nl/game or by self-hosting it with possible adjustments via the code available at https://github.com/fkmke/stegadventure. However, prior knowledge of binary representation is recommended. Additionally, individuals can play the game during their free time to become more familiar with the concept of steganography. However, it is not advisable to promote the game as a quick learning tool for steganography via social media, as its playtime typically ranges from 12 to 25 minutes.

10 ACKNOWLEDGEMENTS

I would like to thank Dr. D.K. Sarmah for her guidance and assistance during this research. I would also like to express my gratitude to Dr. T. Prince Sales and I. Valle Sousa for their continuous feedback throughout the process.

REFERENCES

[1] L. Anderson, D. Krathwohl, and B. Bloom. 2000. A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. https://api.semanticscholar.org/CorpusID:61966728

[2] Michel van Ast, Otto de Loor, Lambrecht Spijkerboer, Sebo Ebbens, and Simon Ettekoven. 2022. *Effectief leren: de docent als regisseur* (vijfde druk ed.). Noordhoff, Groningen. OCLC: 1371480965.

[3] Kayode Ayinde, Taiwo Joel Adejumo, and Gbenga Sunday Solomon. 2016. A study on Sensitivity and Robustness of one sample test Statistics to outliers. *Global Journal of Science Frontier Research (GJSFR)* 16, 6 (2016), 99–112. https://www.researchgate.net/profile/Adejumo-Taiwo-Joel/publication/340579973_A_Study_on_Sensitivity_and_Robustness_of_One_Sample_Test_Statistics_to_Outliers/links/5e91e3c0299bf130798fc86f/A-Study-on-Sensitivity-and-Robustness-of-One-Sample-Test-Statistics-to-Outliers.pdf Publisher: Global Journals Inc. (USA).

[4] Ivan L. Beale, Pamela M. Kato, Veronica M. Marin-Bowling, Nicole Guthrie, and Steve W. Cole. 2007. Improvement in Cancer-Related Knowledge Following Use of a Psychoeducational Video Game for Adolescents and Young Adults with Cancer. *Journal of Adolescent Health* 41, 3 (Sept. 2007), 263–270. https://doi.org/10.1016/j.jadohealth.2007.04.006

[5] Enzo Caminotti and Jeremy Gray. 2012. The effectiveness of storytelling on adult learning. *Journal of Workplace Learning* 24, 6 (Jan. 2012), 430–438. https://doi.org/10.1108/13665621211250333 Publisher: Emerald Group Publishing Limited.

[6] Lais Tono Cardozo, Aline Soares Miranda, Maria José Costa Sampaio Moura, and Fernanda Klein Marcondes. 2016. Effect of a puzzle on the process of students' learning about cardiac physiology. *Advances in Physiology Education* 40, 3 (Sept. 2016), 425–431. https://doi.org/10.1152/advan.00043.2016 Publisher: American Physiological Society.

[7] Meng-Tzu Cheng, Yu-Wen Lin, and Hsiao-Ching She. 2015. Learning through playing *Virtual Age*: Exploring the interactions among student concept learning, gaming performance, in-game behaviors, and the use of in-game characters. *Computers & Education* 86 (Aug. 2015), 18–29. https://doi.org/10.1016/j.compedu.2015.03.007

[8] Meng-Tzu Cheng, Yu-Wen Lin, Hsiao-Ching She, and Po-Chih Kuo. 2017. Is immersion of any value? Whether, and to what extent, game immersion experience during serious gaming affects science learning. *British Journal of Educational Technology* 48, 2 (2017), 246–263. https://doi.org/10.1111/bjet.12386 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/bjet.12386.

[9] Michelene T. H. Chi and Ruth Wylie. 2014. The ICAP Framework: Linking Cognitive Engagement to Active Learning Outcomes. *Educational Psychologist* 49, 4 (Oct. 2014), 219–243. https://doi.org/10.1080/00461520.2014.965823 Publisher: Routledge _eprint: https://doi.org/10.1080/00461520.2014.965823.

[10] Kaustubh Choudhary. 2012. Image Steganography and Global Terrorism. *IOSR Journal of Computer Engineering* 1, 2 (2012), 34–48. https://doi.org/10.9790/0661-0123448

[11] Aviad Cohen, Nir Nissim, and Yuval Elovici. 2020. MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images. *IEEE Access* 8 (2020), 19997–20011. https://doi.org/10.1109/ACCESS.2020.2969022 Conference Name: IEEE Access.

[12] Robert F. DeVellis. 2017. *Scale development: theory and applications* (fourth edition ed.). Number 26 in Applied social research methods series. SAGE, Los Angeles, Calif. London New Delhi Singapore Washington, DC Melbourne.

[13] C. Girard, J. Ecalle, and A. Magnan. 2013. Serious games as new educational tools: how effective are they? A meta-analysis of recent studies. *Journal of Computer Assisted Learning* 29, 3 (2013), 207–219. https://doi.org/10.1111/j.1365-2729.2012.00489.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1365-2729.2012.00489.x.

[14] Dianyuan Han, Jianhua Yang, and Wayne Summers. 2017. Inject Stenography into Cybersecurity Education. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. 50–55. https://doi.org/10.1109/WAINA.2017.30

[15] Winston Hill, Mesafint Fanuel, and Xiaohong Yuan. 2020. Comparing Serious Games for Cyber Security Education. In *Proceedings of the 2020 ASEE Southeastern Section Conference, Auburn, AL, USA*. ASEE, 8–9.

[16] Hyun Kang. 2021. Sample size determination and power analysis using the G*Power software. *Journal of Educational Evaluation for Health Professions* 18, 0 (July 2021), 17–0. https://doi.org/10.3352/jeehp.2021.18.17 Publisher: Korea Health Personnel Licensing Examination Institute.

[17] Amelie Friederike Kanzow, Dennis Schmidt, and Philipp Kanzow. 2022. Scoring Single-Response Multiple-Choice Items: Scoping Review and Comparison of Different Scoring Methods (Preprint). https://doi.org/10.2196/preprints.44084

[18] Mansureh Kebritchi, Atsusi Hirumi, and Haiyan Bai. 2010. The effects of modern mathematics computer games on mathematics achievement and class motivation. *Computers & Education* 55, 2 (Sept. 2010), 427–443. https://doi.org/10.1016/j.compedu.2010.02.007

[19] Gary C. Kessler and Chet Hosmer. 2011. An Overview of Steganography. In *Advances in Computers*, Marvin V. Zelkowitz (Ed.). Vol. 83. Elsevier, 51–107. https://doi.org/10.1016/B978-0-12-385510-7.00002-3

[20] Jang Wan Ko, Sumee Park, Hyun Sook Yu, Seon-Joo Kim, and Dong Min Kim. 2016. The Structural Relationship Between Student Engagement and Learning Outcomes in Korea. *The Asia-Pacific Education Researcher* 25, 1 (Feb. 2016), 147–157. https://doi.org/10.1007/s40299-015-0245-2

[21] Udo Kuckartz, Stefan Rädiker, Thomas Ebert, and Julia Schehl. 2013. *Statistik: Eine verständliche Einführung* (2., überarb. aufl. 2013 ed.). VS Verlag für Sozialwissenschaften, Wiesbaden. https://doi.org/10.1007/978-3-531-19890-3

[22] Kristoffer Magnusson. 2023. A Causal Inference Perspective on Therapist Effects. https://doi.org/10.31234/osf.io/f7mvz

[23] Robert J. Marzano and Wietske Miedema. 2023. *Leren in vijf dimensies: moderne didactiek voor het voortgezet onderwijs* (7e geheel herziene druk ed.). Uitgeverij Koninklijke Van Gorcum, Assen. OCLC: 1445430252.

[24] Muijtjens, H van Mameren, Hoogenboom, Evers, and C P M van der Vleuten. 1999. The effect of a 'don't know' option on test scores: number-right and formula scoring compared. *Medical Education* 33, 4 (1999), 267–275. https://doi.org/10.1046/j.1365-2923.1999.00292.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1046/j.1365-2923.1999.00292.x.

[25] Emily Naul and Min Liu. 2020. Why Story Matters: A Review of Narrative in Serious Games. *Journal of Educational Computing Research* 58, 3 (June 2020), 687–707. https://doi.org/10.1177/0735633119859904 Publisher: SAGE Publications Inc.

[26] Elena Nyemkova, Connie Justice, Solomiia Liaskovska, and Yuriy Lakh. 2022. Methods of Current Knowledge Teaching on the Cybersecurity Example. *Education Sciences* 12, 11 (Nov. 2022), 732. https://doi.org/10.3390/educsci12110732 Number: 11 Publisher: Multidisciplinary Digital Publishing Institute.

[27] Heather L. O'Brien and Lori McCay-Peet. 2017. Asking "Good" Questions: Questionnaire Design and Analysis in Interactive Information Retrieval Research. In *Proceedings of the 2017 Conference on Conference Human Information Interaction and Retrieval (CHIIR '17)*. Association for Computing Machinery, New York, NY, USA, 27–36. https://doi.org/10.1145/3020165.3020167

[28] Heather L. O'Brien and Elaine G. Toms. 2010. The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology* 61, 1 (2010), 50–69. https://doi.org/10.1002/asi.21229 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/asi.21229.

[29] Heather O'Brien and Paul Cairns. 2015. An empirical evaluation of the User Engagement Scale (UES) in online news environments. *Information Processing & Management* 51, 4 (July 2015), 413–427. https://doi.org/10.1016/j.ipm.2015.03.003

[30] Heather L. O'Brien, Paul Cairns, and Mark Hall. 2018. A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. *International Journal of Human-Computer Studies* 112 (April 2018), 28–39. https://doi.org/10.1016/j.ijhcs.2018.01.004

[31] M. Prensky. 2001. Digital Game-Based Learning. *McGraw-Hill, New York* 1 (Jan. 2001). https://doi.org/10.1145/950566.950567

[32] C. J. Ravesloot, M. F. Van der Schaaf, A. M. M. Muijtjens, C. Haaring, C. L. J. J. Kruitwagen, F. J. A. Beek, J. Bakker, J. P. J. Van Schaik, and Th. J. Ten Cate. 2015. The don't know option in progress testing. *Advances in Health Sciences Education* 20, 5 (2015), 1325–1338. https://doi.org/10.1007/s10459-015-9604-2

[33] Maartje Bakhuys Roozeboom, Gillian Visschedijk, and Esther Oprins. 2017. The effectiveness of three serious games measuring generic learning features. *BRITISH JOURNAL OF EDUCATIONAL TECHNOLOGY* 48, 1 (Jan. 2017), 83–100. https://doi.org/10.1111/bjet.12342 Num Pages: 18 Place: Hoboken Publisher: Wiley Web of Science ID: WOS:000393868000007.

[34] Brandon M. Savage, Heidi L. Lujan, Raghavendar R. Thipparthi, and Stephen E. DiCarlo. 2017. Humor, laughter, learning, and health! A brief review. *Advances in Physiology Education* 41, 3 (Sept. 2017), 341–347. https://doi.org/10.1152/advan.00030.2017 Publisher: American Physiological Society.

[35] Jesper Simon. 2023. *A serious game on image steganography training for students in higher education.* info:eu-repo/semantics/bachelorThesis. University of Twente. https://essay.utwente.nl/94438/ StegAware: https://jespersimon.itch.io/stegaware.

[36] Bartosz Sokół and V. N. Yarmolik. 2005. Cryptography and Steganography: teaching experience. In *Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems*, Jerzy Pejaś and Andrzej Piegat (Eds.). Springer US, Boston, MA, 83–92. https://doi.org/10.1007/0-387-23484-5_8

[37] Fabienne M. Van der Kleij, Remco C. W. Feskens, and Theo J. H. M. Eggen. 2015. Effects of Feedback in a Computer-Based Learning Environment on Students' Learning Outcomes: A Meta-Analysis. *Review of Educational Research* 85, 4 (Dec. 2015), 475–511. https://doi.org/10.3102/0034654314564881 Publisher: American Educational Research Association.

[38] Eric N. Wiebe, Allison Lamb, Megan Hardy, and David Sharek. 2014. Measuring engagement in video game-based environments: Investigation of the User Engagement Scale. *Computers in Human Behavior* 32 (March 2014), 123–132. https://doi.org/10.1016/j.chb.2013.12.001

[39] Simon Wiseman. 2017. Stegware – Using Steganography for Malicious Purposes. (2017). https://doi.org/10.13140/RG.2.2.15283.53289

[40] Yu Zhonggen. 2019. A Meta-Analysis of Use of Serious Games in Education over a Decade. *International Journal of Computer Games Technology* 2019, 1 (2019), 4797032. https://doi.org/10.1155/2019/4797032 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2019/4797032.

A LEARNING GOALS INTEGRATION

The learning goals from Section 2 have its main presence in some nodes of the game. How they are related is shown in Table 5.

Table 5. Presence of learning goals from Section 2 in nodes within the story of the game

Learning Goal	**Node(s)**	**Notes**
1	130-135	Basics of cryptography
	241-243	Example and definition of both cryptography and steganography
2	502	The student needs to determine whether to use steganography or cryptography to infiltrate the system
	610	The student needs to determine whether to use steganography, cryptography, or nothing to get sensitive data out of the system
3	333-339	Least Significant Bits (LSB) explanation
	345-347	Example how to hide a message within LSB
	380-381	The student needs to determine what message is hidden within the LSB of the given image
4	520	The student must choose a suitable image to perform steganography on
	521-524	Feedback on the student's choice at node 520
5	230	Example context of people sharing images containing hidden messages
	242-244	Two real-world examples given
	400-401	Example context of using social media and steganography to communicate secretly
6	352-362, 365-375	Example malicious software can be embedded in the image
	500	The student must infiltrate in the enemy's system by acting as StegWare
7	302	Example that cover medium does not necessarily need to be an image
	610	The student must hide in a PDF, trying to imply more covering media than solely images can be used
8	220	The student sees a similar diagram
	221-231	Explanation of the diagram
	300-306	More explanation of the diagram
9	227, 303	Stego key usage explanation
	348-350	Explanation what would have happened if the enemy used a stego key
10	356, 369	Relation Intrusion Detection System (IDS) and steganography
	502	The student needs to determine whether to use steganography or cryptography to infiltrate the system
	610	The student needs to determine whether to use steganography, cryptography, or nothing to get sensitive data out of the system
11	406, 407, 410-411	Introduce the term StegWare
	412-433	Propose the plan to intrude the enemy's network, which the player must carry out from node 500 onwards

Table 6. Modified User Engagement Scale for Group A

UES sub-scale	Question
FA-S.1	I lost myself in this gaming experience.
FA-S.2	The time I spent playing the game just slipped away.
FA-S.3	I was absorbed in my gaming task.
PU-S.1	I felt frustrated while playing the game.
PU-S.2	I found the game confusing to use.
PU-S.3	Using the game was mentally demanding.
AE-S.1	The game was attractive.
AE-S.2	The game was aesthetically appealing.
AE-S.3	The game appealed to my visual senses.
RW-S.1	Playing the game was worthwhile.
RW-S.2	My gaming experience was rewarding.
RW-S.3	I felt interested in this gaming experience.

Table 7. Modified User Engagement Scale for Group B

UES sub-scale	Question
FA-S.1	I lost myself in this reading experience.
FA-S.2	The time I spent reading the text just slipped away.
FA-S.3	I was absorbed in my reading task.
PU-S.1	I felt frustrated while reading the text.
PU-S.2	I found the text confusing.
PU-S.3	Reading the text was mentally demanding.
AE-S.1	The text was attractive.
AE-S.2	The text was aesthetically appealing.
AE-S.3	The text appealed to my visual senses.
RW-S.1	Reading the text was worthwhile.
RW-S.2	My reading experience was rewarding.
RW-S.3	I felt interested in this reading experience.

B USER ENGAGEMENT SCALE SHORT FORM (UES-SF)

Tables 6 and 7 present the questions asked to Group A and Group B regarding their engagement with the task they performed. These questions were adapted for context, following the guidelines of O'Brien et al. (2018) [30]. Additionally, inspiration was drawn from Wiebe (2014), who proposes a reliable scale for assessing gaming experience [38].

Minor adjustments were made for clarity. For instance, the term "taxing" was replaced with "demanding" to enhance understanding. Furthermore, to avoid confusion, references to both "the website" and "the game" in a single UES were removed, as these were present in the UES used by Wiebe (2014). In this study, the UES-SF consistently uses references to either "the game" or "the text," and does not mention "the website."

C COMMENTS BY PARTICIPANTS

The received comments about the game and steganography text have been categorised. The categorised comments about the game can be found in Table 8 and the comments about the steganography text can be found in Table 9.

Table 8. Comments made about the game by participants after the experiment (Group A)

Aesthetics and feeling	
1	The art was amateurish, but it's still a nice game (2×)
2	Some fonts were not nice to read (1×)
3	Add sound effects and music (2×)
4	Great story (1×)
5	The visuals were visually pleasing (1×)
Explanation	
6	Difference between cryptography and steganography was not clear (1×)
7	Better advice on which image is the best image to choose for steganography (1×)
8	How to find the message in the LSB was unclear (3×)
Other	
9	It was fun (6×)
10	Some questions could be harder (1×)
11	Game was too long (1×)
12	It was frustrating to not have an option to read back the text (1×)
13	There was a high information density in a short amount of time (2×)
14	Fun responses and the jokes were a nice addition (2×)
Bugs	
15	Images were not loading (1×)

Table 9. Comments made about the steganography text by participants after the experiment (Group B)

Aesthetics and feeling	
1	Add more visual examples (1×)
2	The images were helpful (1×)
3	Dark mode would be great (1×)
Explanation	
4	The part about the stego key was boring (1×)
5	Some topics on the test were not covered in the text (1×)
6	I did not understand StegWare very well (1×)
7	How to find the message in the LSB was unclear (1×)
8	More (real-life) examples would be nice (2×)
Other	
9	English improvements would be nice (3×)
10	The text was a good read (4×)
11	Some information was outdated (1×)

D SERIOUS GAMES ON STEGANOGRAPHY COMPARISON

Both our study and Simon (2023) [35] implemented and validated a serious game focused on steganography, evaluating user engagement and knowledge acquisition. Table 10 presents a comparison of the methodologies and conclusions from both studies.

Table 10. Table comparing two serious games on steganography

	StegAdventure (our game)	**StegAware [35]**	**Notes**
Game type	Narrative-based serious game.	Quiz-based serious game.	
Participants	54 participants, primarily higher educated individuals aged 18–30, with a small number over 30.	15 university students aged 18–24.	StegAdventure includes a slightly older participant group, with two individuals aged above 30.
Learning goals	Introduction to steganography, primarily aimed at a classroom setting.	Raising awareness of steganography, with a focus on attack prevention.	The content covered is largely similar, but StegAware includes slightly more advanced topics, such as file types, which are not addressed in StegAdventure.
User engagement test methodology	Used the User Engagement Scale Short Form (UES-SF), and comparing mean scores with a two-sample t-test against a control group.	Asked a single question, "The game kept me engaged," on a Likert scale, comparing the mean to the neutral midpoint (3) using a one-tailed t-test and a one-sample Wilcoxon signed-rank test.	StegAdventure employs a comprehensive, validated engagement scale (UES-SF), whereas StegAware relies on a single Likert-scale question, which provides less detailed insight into user engagement.
Engagement conclusion	Found a significant difference in engagement between the game group and the control group (text readers), with a power of 0.7061.	Did not find a significant increase in engagement, with a power of 0.2136.	The power for StegAware was calculated based on the reported participant count (n = 15) and t-value (t = 0.851). Using the formula $d = \frac{t}{\sqrt{n}} = \frac{0.851}{\sqrt{15}} = 0.2197$, the Cohen's effect size was determined. This effect size was input into the Statistics Kingdom tool[a] to compute the power.
Acquired knowledge test methodology	Used a peer-reviewed knowledge test to assess learning outcomes, comparing the means of test scores between the game group and the control group (text readers) using a two-sample t-test.	Assessed learning through self-reported measures by asking "I feel that my awareness in cybersecurity has increased." and "I feel that my awareness on steganography has increased." Responses were on a Likert scale, compared to the neutral midpoint (3) using a one-tailed t-test and a one-sample Wilcoxon signed rank test. Additionally, participants were asked the yes/no question: "Did you learn something from the game?"	The two methodologies differ significantly: StegAdventure relies on an objective knowledge test, directly measuring learning outcomes, while StegAware uses self-perception-based questions, which reflect subjective impressions of learning rather than objective knowledge acquisition.
Acquired knowledge conclusion	Found no significant difference between the reading group and the game group in test scores. This conclusion was reached with a low power of 0.3045, indicating limited sensitivity to detect differences. However, the mean and median test scores for both groups were above the sufficient grade threshold in the Netherlands, suggesting that most participants achieved the learning objectives.	Reported a significant increase in self-reported cybersecurity knowledge (power = 0.9842) and steganography knowledge (power = 1.0000). Additionally, 100% of participants stated that they learned something from the game.	The difference in methodologies makes it challenging to directly compare the effectiveness of the two games in facilitating knowledge acquisition. The power of StegAware's findings was calculated using reported t-values, Cohen's effect size $d = \frac{t}{\sqrt{n}}$ and Statistics Kingdom's tool[a].

[a]Tool used: https://www.statskingdom.com/32test_power_t_z.html

E AI STATEMENT

During the preparation of this work, I used ChatGPT to help me with converting my written sentences to academic language. I have never asked the service to generate new text for me for this work. I also used ChatGPT to generate code or find bugs in my code while creating the experiment environment and the graphs for data analysis. ChatGPT never received any participant data.

Additionally, I used Adobe Firefly to generate background images for the game to improve aesthetics. Other images used in the experiment, are either licensed to be able to used in this project, or have been drawn by myself.

After using these services, I thoroughly reviewed and edited the content as needed, taking full responsibility for the final outcome.