AN INTERACTIVE VISUALIZATION TOOL FOR ANIMATING BEHAVIOR OF CRYPTOGRAPHIC PROTOCOLS

Mabroka Maeref[1], Fatma Algali[2], Ahmed Patel[3] and Zarina Shukur[4]

[1]Department of Computer Science, Sebha University, Sebha, Libya
[2]Department of Computer Science, Sebha University, Sebha, Libya
[3]Faculty of Technology and Information Science, The National University of Malaysia, Kuala Lumpur, Malaysia
[4]Faculty of Technology and Information Science, The National University of Malaysia, Kuala Lumpur, Malaysia

ABSTRACT

Cryptography and Network Security is a difficult subject to understand, mainly because of the complexity of security protocols and the mathematical rigour required to understand encryption algorithms. Realizing the need for an interactive visualization tool to facilitate the understanding of cryptographic concepts and protocols, several tools had been developed. However, these tools cannot be easily adapted to animate different protocols. The aim of this paper is to propose an interactive visualization tool, called the Cryptographic Protocol Animator (CPAnim). The tool enables a student to specify a protocol and gain knowledge about the impact of its behavior. The protocol is specified by using a scenario-based approach and it is demonstrated as a number of scenes displaying a complete scenario. The effectiveness of this tool was tested using an empirical evaluation method. The results show that this tool was effective in meeting its learning objectives.

KEYWORDS

Cryptographic Protocols, Visualization and Animation, Scenario-based Approach, Empirical Evaluation

1.INTRODUCTION

The visualization and animation approach is increasingly being adopted in Computer Science education with the promise of enhancing student understanding of complex concepts. Using this approach, tools were developed using visualization and animation techniques to interactively help students gain knowledge and acquire skills about a subject. If these tools are exploited efficiently, they can facilitate the education process, thus minimizing the learning/teaching time for both lecturers and students.

In the area of network security, fundamental security principles and security practice skills are both required for a student to understand the subject matter. Instructors have to emphasize both the theoretical and practical aspects of security. However, this area poses a challenge for instructors to teach and for students to learn. For this reason, researchers have been eager to support lectures by offering interactive visualization and animation tools that facilitate student understanding and shorten the time consumed in long-term teaching [1-8].

DOI : 10.5121/ijnsa.2015.7202

In response to the rising number of security crimes and attacks, specific security courses have been developed by colleges and universities[9]. Although the Model Curricula for Computing CC-2008[10] describes a cryptographic algorithm as an elective unit–[10] with topics that include private and public key cryptography, key exchanges, digital signatures and security protocols– security experts, including Bishop[11], Hoglund[12] and Howard [13], emphasize the need to incorporate security into the undergraduate curriculum.

Cryptographic protocols mostly combine both theory and practice[14,15] and as such, interactive visualization tools are essential [7,8] to support a student's understanding of the subject matter. In fact, Adding reality, with the help of realistic images and colors, offers a better chance of enhancing student understanding of protocol behavior. If objects in the animation can be moved and transferred around, this would ensure better understanding and knowledge retention [16,17]. This feature is missing in most current interactive visualization tools and the quest for the appropriate tool is still open to research.

In this paper, we propose an interactive visualization tool called CPAnim which uses visual images from the real world to reflect the object characteristics. It also describes the protocol behavior as a scenario to enable students to formalize the given protocol behavior. The tool is evaluated using an empirical evaluation approach and compared with another chosen tool called a CrypTool 2 [18] to determine the quality of both tools. The following section describes the most related works to our paper while section 3 explains the proposed CPAnim tool. Tools evaluation and results are described in section 4. Section 5 describes the comparison between CrypTool and CPAnim tools. A discussion of this paper is explained in section 6 and the conclusion is provided in section 7.

2. RELATED WORK

Researchers have developed various kinds of interactive visualization tools for teaching/learning cryptographic protocol behaviour and concepts. One of these tools is the Kerberos tool, which developed for visualizing one specific protocol: Kerberos protocol[19]. Another tool is the GRACE tool [3], the Game tool [20], GRASP tool [21] and crypTool[22,23]. CrypTool is a freeware Program with graphical user interface for applying and analyzing cryptographic algorithms with extensive online help. Literature on related visualization tools, together with comparisons between them, is available in our papers [24] and [25].

The main goal of this paper is to propose an interactive visualization tool (CPAnim) and to evaluate quantitatively the effectiveness of this tool and other chosen tool which is CrypTool. For the purpose of this paper, effectiveness refers to the ability of these tools in enhancing student's understanding. This goal is evaluated using an empirical evaluation approach (without animation vs. animation with CPAnim tool vs. animation with CrypTool tool). We have chosen this tool for comparison because it covers the most aspects of computer security. With respect to this chosen tool, the questions are, "*Is teaching using interactive visualization tools more effective than traditional teaching medium?*" and "*Is teaching using CPAnim tool more effective than CrpTool tool?*".

Various studies have been carried out for evaluating interactive mediums. From the literature, a study conducted by Kehoe et al.[26] used an interactive animation to teach algorithm animation and data structure. Their results showed in scores on a post-test used to evaluate the understanding with 12 students divided into two groups. The results showed that the animation group significantly outperformed the non animation group. Moreover, Yuan et al.[8] used Kerberos as an interactive animation tool to teach Kerberos protocol. His results showed in scores on pre-post tests used to evaluate the understanding with 16 students. The *t*-test results show that the improvement from pre-test to post-test is statistically significant. Hundhausen et al. [27] also considered 24 experiments used different concept of animation to teach algorithm animation and data structures. Twenty two of the experiments used post-test or pre-post tests to evaluate the understanding. Their results are various according to the interactivity of animation.

3. The Proposed CPAnim Tool

Our objectives of evaluating the CPAnim visualization tool are:

[1] To minimize protocol complexity by separating the mathematical part from the protocol behavior. A student should feel how the protocol works, thus increasing student's ability to understand and to gain confidence in accepting more complicated information, as well as to generate interest to know about other more complex protocol concepts.
[2] To improve student comprehension of cryptographic protocol concepts and behavior. Animation can make such concepts appear more structured and realistic.
[3] To enhance student understanding of the foundation of cryptographic protocols. This foundation can be used to better understand modern cryptographic protocol concepts, and how these protocols work.
[4] To increase student retention of knowledge by providing the same concepts both textually and visually. Experiencing two different learning approaches to the same subject can improve student understanding.

The CPAnim tool provides a high degree of interactivity by enabling these features:

- The ability to “backup” a step to see what just happened and be able to replay it. The CPAnim tool provides this feature such that each protocol consists of one or more scenes, and each scene consists of a number of actors and processes. Using the scenario-based approach, it is possible to backup a protocol scenario in a file and play back this scenario by just re-running previously executed scenes.
- The possibility to record the contents of visualization by just saving the list of scenes in a file. Each process is accompanied by a text description that explains and comments on the process to aid comprehension.
- The capability to be paused at any point, to allow the instructor to answer questions or to explain a concept.
- The capability to navigate around the different scenes of the visualization.
- Control buttons, such as “Stop”, “Forward” and “Pause” to ensure effective interaction with the animated learning.

3.1. Example Interaction

This section describes Diffie-Hellman protocol [15]. In this protocol, two parties create a symmetric session key. Before doing so, they need to choose two numbers, p and g, which do not need to be confidential. These numbers can be sent through the internet and can be made public.

The steps are as follows:

1. Alice chooses a large random number, x, such that 0=< x <=p-1, and calculates R1= g^x mod p.

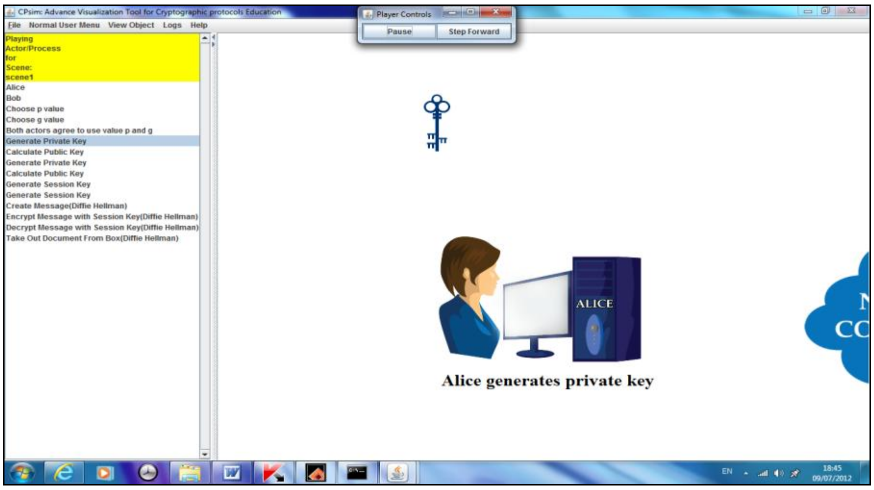
2. Bob chooses another large random number, y, such that 0=< y <=p-1, and calculates R2= g^y mod p.
3. Alice sends R1 to Bob. Note that Alice does not send the value of x; she sends only R1.
4. Bob sends R2 to Alice. Note that Bob does not send the value of y; he sends only R2.
5. Alice calculates K=$[R2]^x$ mod p.
6. Bob also calculates K=$[R1]^y$ mod p

} where K is the symmetric key for the

3.2. Visualization of Diffie-Hellman Protocol

In order to visualize the Diffie-Hellman protocol using CPAnim tool, the user has to first select the two actors (Alice and Bob) designated to run the key agreement protocol. Each actor has a unique color code (Alice is blue and Bob is brown). Then, the user constructs the scenes by choosing the processes that are related to the Diffie-Hellman protocol under the process options. Any generated key has the same color as the creator of this key. For example: Alice's private and public keys are blue. Finally, an actor can swap his/her own public keys with those of the other actor, or get a copy of the public key which belongs to any other actor and combines it with his/her own private key. The combination of the two keys will result in the generation of a new secret key (black key). Once generated, the new symmetric key can be used by the actor to encrypt a message and send it to another actor.

The idea behind the CPAnim visualization of the Diffie-Hellman protocol lies in separating the mathematical part from the protocol behavior in order to minimize protocol complexity, thereby making the steps easier to understand. A student should feel how the protocol works, thus increasing his/her ability to understand it and to gain confidence in accepting more complex information. Below are the important parts of CPAnim's Diffie-Hellman protocol demonstration (Figures 1, 2, 3 and 4).



Playing
Actor/Process
for
Scene:
scene1
Alice
Bob
Choose p value
Choose g value
Both actors agree to use value p and g
Generate Private Key
Calculate Public Key
Generate Private Key
Calculate Public Key
Generate Session Key
Generate Session Key
Create Message(Diffie Hellman)
Encrypt Message with Session Key(Diffie Hellman)
Decrypt Message with Session Key(Diffie Hellman)
Take Out Document From Box(Diffie Hellman)

Alice generates private key

Figure 1. Alice generates her private key

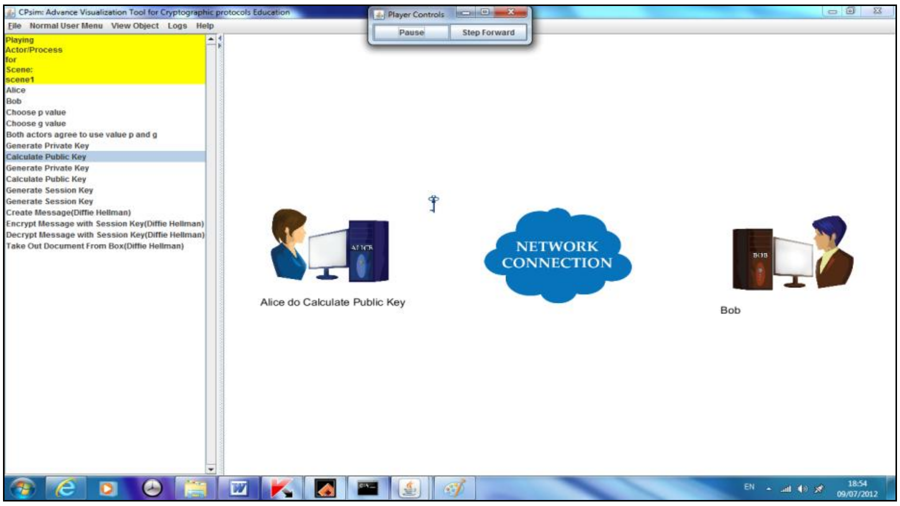


Figure 2. Alice generates her public key and sends it to Bob

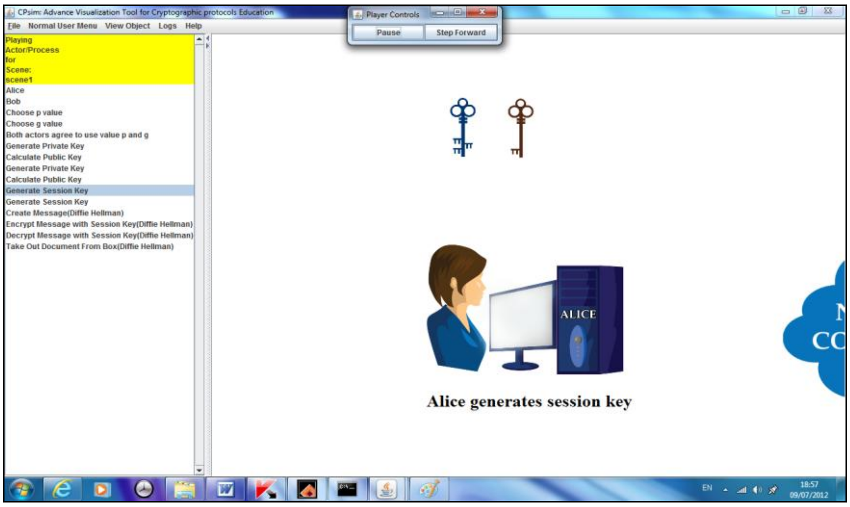

CPsim: Advance Visualization Tool for Cryptographic protocols Education
File
Normal User Menu
View Object
Logs
Help
Player Controls
Pause
Step Forward
Playing
Actor/Process
for
Scene:
scene1
Alice
Bob
Choose p value
Choose g value
Both actors agree to use value p and g
Generate Private Key
Calculate Public Key
Generate Private Key
Calculate Public Key
Generate Session Key
Generate Session Key
Create Message(Diffie Hellman)
Encrypt Message with Session Key(Diffie Hellman)
Decrypt Message with Session Key(Diffie Hellman)
Take Out Document From Box(Diffie Hellman)
ALICE
Alice generates session key
N
CC
EN
18:57
09/07/2012

Figure 3. Alice combines her private key with Bob’s public key

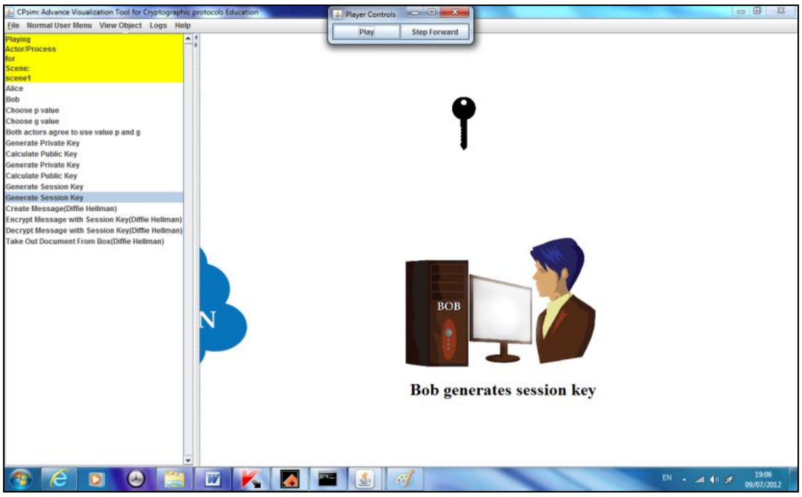

CPsim: Advance Visualization Tool for Cryptographic protocols Education
File
Normal User Menu
View Object
Logs
Help
Player Controls
Play
Step Forward
Playing
Actor/Process
for
Scene:
scene1
Alice
Bob
Choose p value
Choose g value
Both actors agree to use value p and g
Generate Private Key
Calculate Public Key
Generate Private Key
Calculate Public Key
Generate Session Key
Generate Session Key
Create Message(Diffie Hellman)
Encrypt Message with Session Key(Diffie Hellman)
Decrypt Message with Session Key(Diffie Hellman)
Take Out Document From Box(Diffie Hellman)
N
BOB
Bob generates session key
EN
19:06
09/07/2012

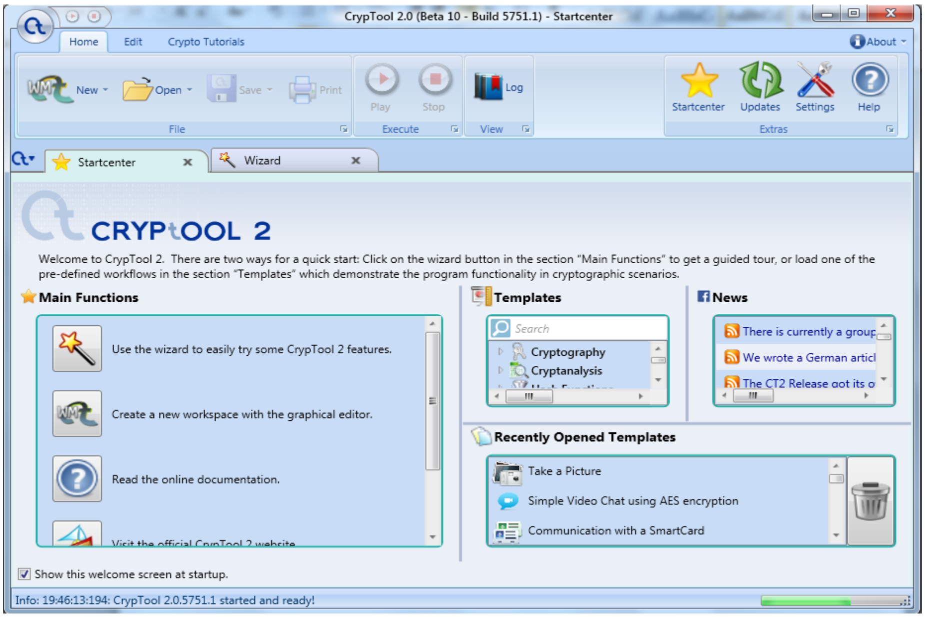
Figure 4. Bob generates the session key

4. TOOLS EVALUATION

The effectiveness of the CPAnim tool is evaluated using an empirical evaluation method[8,26-28] and comparing the CPAnim tool against another existing tool, namely CrypTool. Two experiments were conducted to compare the two tools. The mathematical element of cryptography is not evaluated in this paper, as our focus is on the visualization and animation of protocols behaviors. This section defines the tools descriptions including the guidelines for selecting the chosen tool to be compared with, the subject of the lesson used in the experiments, and the experiments results.

4.1. CrypTool Description

Cryptool is a freeware Program with graphical user interface for applying and analysing cryptographic algorithms with extensive online help. It can be understandable without deep crypto knowledge. It contains nearly all state of the art crypto algorithms with "playful" introduction to modern and classical cryptography. Learning through CrypTool is almost can be done by everyone either through the internet or by download and install the tool from the website (www.cryptool.org). The features of CrypTool include cryptography and cryptanalysis. Both of them constitute the science of cryptology. Figure 5 shows the main menu of the tool.



CrypTool 2.0 (Beta 10 - Build 5751.1) - Startcenter

Welcome to CrypTool 2. There are two ways for a quick start: Click on the wizard button in the section "Main Functions" to get a guided tour, or load one of the pre-defined workflows in the section "Templates" which demonstrate the program functionality in cryptographic scenarios.

Use the wizard to easily try some CrypTool 2 features.

Create a new workspace with the graphical editor.

Read the online documentation.

Visit the official CrypTool 2 website

☑ Show this welcome screen at startup.

Info: 19:46:13:194: CrypTool 2.0.5751.1 started and ready!

Figure 5. CrypTool main menu

In selecting the tool for comparison, two issues had to be considered. The first issue was, "*Is the tool intended for the same type of application?*" It may be unfair to compare tools that are specific to different domains of application, since they may be approaching the matter from different perspectives. The second issue was, "*Does the tool have similar goals?"* Comparing tools with different goals does not do justice to the true ability of each tool to perform and may consequently lead to an unfair judgment. Based on that, it's clear that CrypTool tool intends for the same type of application which is computer security and cryptography and it has the same goal which is enhancing the student understanding of the same subjects.

4.2. CrypTool Evaluation

We carried out the first experiment consists of one group of the same lesson taught to the undergraduate Computer Science students of the Network Security course at Sebha University of Libya during the semester II of 2013-2014 year. The experiment was conducted in two stages where each stage uses a different learning medium approach; the first stage uses only text-based materials (no animation), the second stage uses CrypTool in the final part of the lesson. The student will be given a same test throughout the two stages. They are allowed to improve their answer after each stage. The results of the tests after each stage of the medium approach are compared.

The same topics of the lessons are given during all of the two stages. These topics are: symmetric-key and Asymmetric-key cryptographic protocol, Diffie-Hellman protocol with respect to the possible attack to Diffie-Hellman protocol, the concept of hash function, digital signature and digital certificate.

In this experiment, the tool SPSS [29] is used to statistically evaluate the effectiveness of CrypTool using t-test and p-value.

4.2.1. Experimental Procedure

A total of 20 students participated in the experiment. The students are final year of Computer Science students (undergraduate students) at Sebha University of Libya. We follow the pre-test to post-test accuracy [8,27,30] in order to evaluate the effectiveness of CrypTool. The same students were given the same lesson but using different medium each time. The experiment was conducted using the learning medium approach (no animation vs. animation with CrypTool). The students were given the lesson using only text-based materials followed by a pre-test, then, the same students were introduced to CrypTool followed by a post-test.

The experiment was controlled by delivering the same lesson to all of the students by the same teacher during the two consecutive sessions. The topics were: symmetric-key and Asymmetric-key cryptographic protocol, Diffie-Hellman protocol with respect to the possible attack to Diffie-Hellman protocol and the concept of hash function, digital signature and digital certificate.

In the first session of the three hours, only text-based materials were used during the lesson time with the help of electronic slides. At the end of the session, the students were given a pre-test of ten multiple choice questions with a time limit of 30 minutes to answer them.

In the second session, after the pre-test, students were introduced to CrypTool and to its visual interface. They were asked to experiment with simple symmetric and asymmetric-key cryptographic protocols and to recreate Diffie-Hellman protocol. They were also asked to experiment with the concepts of hash function, digital signature, digital certificate and their usages of avoiding possible attack. At the end of the session, the students were given a post-test of the same questions as in the first session with a time limit of 30 minutes to answer them.

Again, to control the tasks performance, the same test of ten multiple questions were given to all students with a specific time. During the test, the students were not allowed to consult books or use any materials. Then the results of pre-test and post-tests were compared. The following points describe the details of the ten multiple questions:

- The first question dealt with the communication components of asymmetric-key cryptographic protocol.
- The second question dealt with the differences between symmetric-key and asymmetric-key cryptography.
- The third question dealt with Diffie-Hellman protocol steps.
- The fourth question dealt with the communication components of Diffie-Hellman protocols.
- The fifth question dealt with digital signature.
- The sixth question dealt with digital certificate.
- The seventh question dealt with Diffie-Hellman possible attack.
- The eighth question dealt with a hash function.
- The ninth question dealt with avoiding Diffie-Hellman protocol attack.
- The last question dealt with a hybrid system (using of both symmetric and asymmetric-key cryptography).

4.2.2. Experimental Results

To determine the effectiveness of CrypTool, a pre-test and post-test accuracy is used. Table 1 describes the students' scores for the pre-test and post-tests. Notice that the maximum score for each student is 10. In the other side, the Table 2 describes the mean of the group tested and Figure 6 explains the idea.

Table 1. The students' scores of pre-test and post-test

No.	**Pre-test scores No animation**	**Post-test scores Using CrypTool**
1	4	6
2	4	6
3	5	5
4	4	6
5	4	4
6	5	5
7	5	5
8	5	7
9	4	7
10	4	5
11	4	6
12	5	7
13	4	6
14	4	4
15	4	4
16	5	5
17	5	5
18	5	7
19	4	7
20	5	7

Table 2. The students' scores means of pre-test and post-test

Time	Treatment	No.	Mean
Sebha University	No animation	20	4.45
	CrypTool	20	5.70

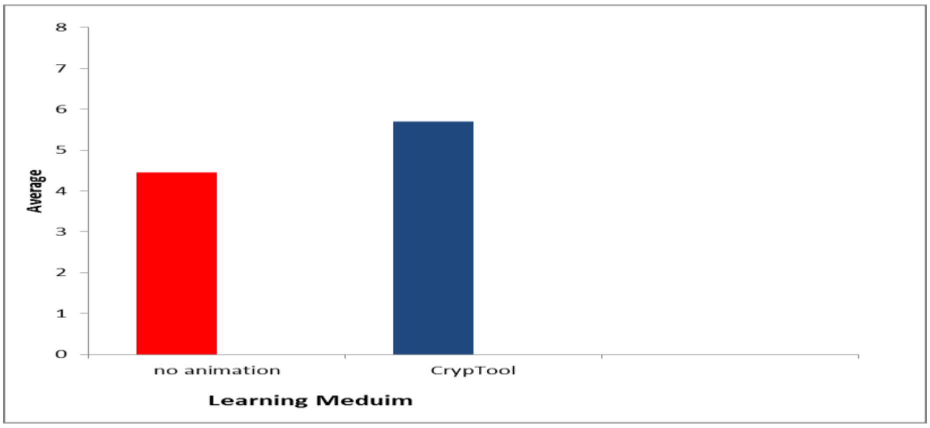


Figure 6. The means of the students' scores

The adopted statistical analysis of this experiment is that:

- Null Hypothesis *(H_0)*: the conducted hypothesis is that there is no difference in the mean of pre-test and post-tests scores. In other words, the pre-test and post-tests scores will have equal means.
- Alternative hypothesis *(H_1)*: the alternative hypothesis is that there is at least one difference in the mean of the pre-test and post-test scores in the group tested.
- p-value: the return value of the statistical test which indicates the probability of getting a mean difference between the groups as high as what is observed by chance. The lower the P-value, the more significant difference between the groups. The typical significance level that has been chosen in this experiment is 0.05.
- t-test: this test was run on the pre-test and post-test scores. In this experiment, the result t-test shows that there is a difference between the pre-test and post-test according to the p-value which is 0.0 and less than the significance level 0.05. Table 3 shows the result of t-test.

Table 3. The results of t-test

Treatment	No. of student	Mean	p-value	t- test
CrypTool No animation	20 20	5.7 4.45	0.0	CrypTool > No animation

The test shows that there is a difference between no animation and CrypTool based on the p-value which equal to 0.0. The p-value is less than the significance level (0.05) and that means the improvement from pre-test to post-test is statistically significant.

4.3. CPAnim Tool Evaluatio

The second experiment procedure is the same as the first experiment but with different group of students at the same University and same course and semester. The tested tool in this second experiment is CPAnim tool.

4.3.1. Experimental Procedure

The same procedure of the first experiment is followed in the second experiment with different group of 20 students. The students are final year of Computer Science students (undergraduate students) at Sebha University of Libya. We follow the same statistical procedure of the first experiment to evaluate the effectiveness of CPAnim Tool.

4.3.2. Experimental Results

To determine the effectiveness of CPAnim Tool, a pre-test and post-test accuracy is used. Table 4 describes the students' scores for the pre-test and post-tests. Notice that the maximum score for each student is 10. In the other side, the Table 5 describes the mean of the group tested and Figure 7 explains the idea.

Table 4. The students' scores of pre-test and post-test

No.	**Pre-test scores** **No animation**	**Post-test scores** **Using CPAnimTool**
1	3	7
2	4	6
3	4	6
4	7	8
5	5	6
6	4	4
7	4	4
8	5	5
9	5	6
10	4	6
11	3	5
12	5	5
13	3	4
14	3	7
15	4	6
16	5	6
17	5	7
18	4	6
19	4	5
20	6	8

Table 5. The students' scores means of pre-test and post-test

Time	**Treatment**	**No.**	**Mean**
Sebha University	No animation	20	4.35
	CPAnim Tool	20	5.85

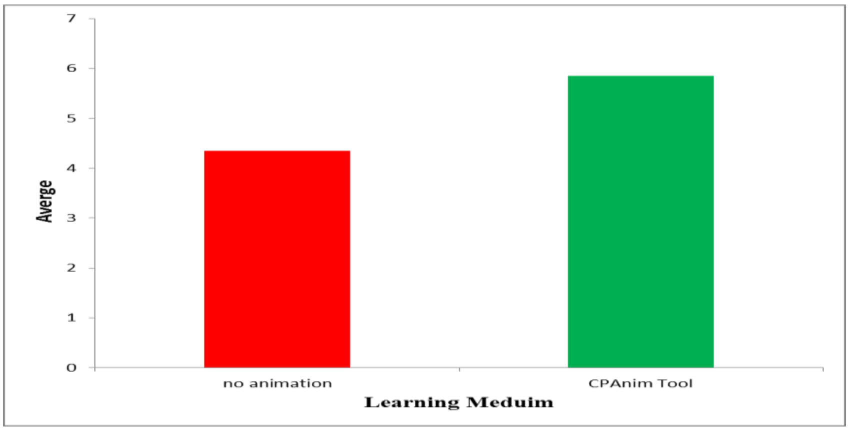


Figure 7. The means of the students' scores

The adopted statistical analysis of this experiment is same as the first experiment. Table 6 shows the result of t-test.

Table 6. The results of t-test

Treatment	No. of student	Mean	p-value	t- test
CPAnim Tool	20	5.85	0.00	CPAnimTool > No animation
No animation	20	4.35		

The test shows that there is a difference between no animation and CPAnim Tool based on the p-value which equal to 0.0. The p-value is less than the significance level (0.05) and that means the improvement from pre-test to post-test is statistically significant.

5. The Comparison Between The First and Second Experiment

In order to determine whether there is a difference in the effectiveness of the CrypTool tool and the CPAnim tool between the students of the first experiment and the students of the second experiment, we ran t-test again on the post-test results of the two experiments. The t-test results show that there is no difference between them, based on the p-value of 0.678. The p-value, which is greater than the significance level 0.05, indicates that no significant difference was found. Table 7 shows the scores of the post-tests of the first and second experiments whilst Table 8 shows means. The results of t-test are shown in Table 9 and Figure 8 illustrates the result graphically.

Table 7. The students' scores of post-tests

No.	Post-test scores Using CrypTool	No.	Post-test scores Using CPAnimTool
1	6	1	7
2	6	2	6
3	5	3	6
4	6	4	8
5	4	5	6
6	5	6	4
7	5	7	4
8	7	8	5
9	7	9	6
10	5	10	6
11	6	11	5
12	7	12	5
13	6	13	4

14	4	14	7
15	4	15	6
16	5	16	6
17	5	17	7
18	7	18	6
19	7	19	5
20	7	20	8

Table 8. The students' scores means of pre-test and post-test

Time	Treatment	No.	Mean
Sebha University	CrypTool Tool	20	5.70
	CPAnim Tool	20	5.85

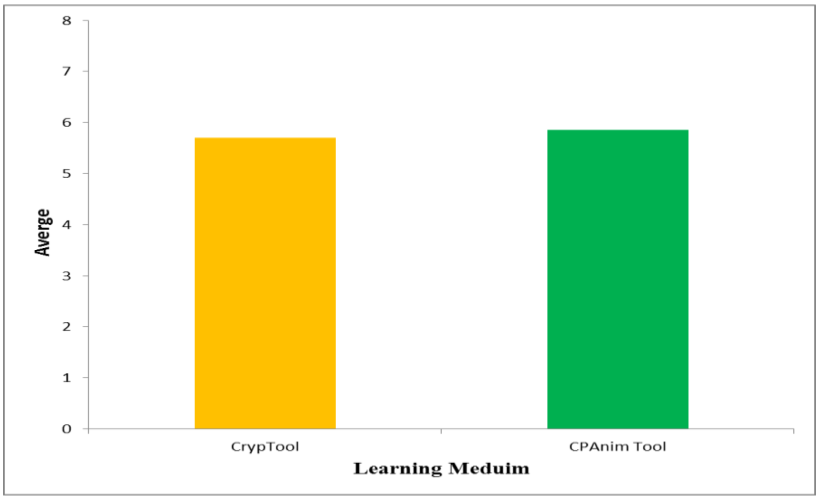


Figure 8. The means of the students' scores

Table 9. The results of t-test

Treatment	No. of student	Mean	p-value	t- test
CrypTool Tool CPAnim Tool	20 20	5.70 5.85	0.678	CrypTool = CPAnimTool

6. DISCUSSION

The results of the first and second experiments prove that the CrypTool and CPAnim tools are more effective than the traditional teaching/learning (no animation). Based on our test of the two hypotheses, there are indeed significant differences between using interactive visualization tools (CrypTool and CPAnim tools) and no animation. In the other side, there is no significant difference between the two tools. both tools contributed positively to learning. Other existing tools could not be evaluated in this paper due to their non-availability and/or difficulty in getting the correct version. The overall improvement of enhancing the students' ability for understanding the cryptographic protocols and computer security concepts using CrypTool and CPAnim tools is demonstrated and achieved.

7. CONCLUSION

Regardless of the advancement in the area of educational techniques, the area needs to be further tested with more empirical evaluation, especially of using the teaching/learning interactive visualization and animation tools. Currently, a few researches dealt with the problem of the lack of using these kinds of tools. The missing of a clear and complete principle design for interactive tools is seldom discussed and yet plays a crucial role in the tool development. The principle design is important because a tool without a base is inadequate even if it is supplied with good structures. Furthermore, studies have shown that visualization and animation educationally enhanced students' understanding if they were supported by active learning. This paper was motivated by these observations. In particular, this paper suggested more experiments of other interactive visualization tools through empirical evaluation in order to improve their effectiveness and teaching/learning support.

REFERENCES

[1] M. S. Asseisah, H. M. Bahig, and S. S. Daoud, Interactive Visualization System for DES. Berlin Heidelberg: Springer-Verlag 2010.

[2] R. Catrambone and A. F. Seay, "Using Animation to Help Students Learn Computer Algorithms," The Journal of the Human Factors and Ergonomics Society, vol. 44, pp. 495-511, 2002.

[3] G. Cattaneo, A. D. Santis, and U. F. Petrillo, "Visualization of cryptographic protocols with GRACE," Journal of Visual Languages and Computing, vol. 19 pp. 258-290, 2008.

[4] M. A. Holliday, "Animation of computer networking concepts," ACM Journal on Educational Resources in Computing (JERIC), vol. 3, pp. 1-26, 2003

[5] N. Kazemi and S. Azadegan, "IPsecLite: a tool for teaching security concepts," in SIGCSE '10 Proceedings of the 41st ACM technical symposium on Computer science education NY, USA, 2010.

[6] A. Kerren and J. T. Stasko, "Algorithm animation," Software Visualization, LNCS 2269, pp. 1-15, 2002.

[7] D. Schweitzer and W. Brown, "Using Visualization to Teach Security," JCSC, vol. 24, pp. 143-150, 2009.

[8] X. Yuan, P. Vega, Y. Qadah, R. Archer, H. Yu, and J. Xu, "Visualization Tools for Teaching Computer Security," ACM Transactions on Computing Education, vol. 9, pp. 147-155, 2010.

[9] B. Taylor and S. Azadegan, "Moving Beyond Security Tracks: Integrating Security in CS0 and CS1," in SIGCSE '08: Proceedings of the 39th SIGCSE technical symposium on Computer science education, 2008, pp. 320-324.

[10] CC2008, "Computer Science 2008, An Interim Revision of CS 2001."

[11] M. Bishop and D. Frincke, "Teaching Secure Programming," IEEE Security and Privacy, vol. 3, pp. 54-56, 2005.

[12] G. Hoglund and G. McGraw, Exploiting Software:How to Break Code. Boston: Addison-Wesley, 2004.

[13] M. Howard and D. LeBlanc, Writing Secure Code. Redmund, WA: Microsoft Press, 2003.

[14] W. Stallings, Cryptography and Network Security: Principles and Practices, 4 ed. Upper Saddle River, NJ: Prentice Hall, 2006.

[15] B. A. Forouzan, Cryptography and Network Security, 1 ed. New York, NY: McGraw-Hill Higher Education, 2008.

[16] L. Lin and R. K. Atkinson, "Using animations and visual cueing to support learning of scientific concepts and processes," Computers & Education, vol. 56, pp. 650-658, 2011.

[17] D. Matthew, H. Timothy, and R. Ingrid, "Using simulation across the curriculum," J. Comput. Small Coll., vol. 16, pp. 56-64, 2000.

[18] A. Deutsche, "CrypTool," 2009.

[19] X. Yuan, Y. Qadah, J. Xu, H. Yu, R. Archer, and B. Chu, "An animated learning tool for Kerberos authentication architecture," Journal of Computing Sciences in Colleges, the twelfth annual CCSC Northeastern Conference, vol. 22, pp. 147 – 155, June 2007 2007.

[20] L. G. C. Hamey, "Teaching Secure Communication Protocols Using a Game Representation," in Australasian Computing Education Conference (ACE2003), Adelaide, Australia, 2002.

[21] D. Schweitzer, L. Baird, M. Collins, W. Brown, and M. Sherman, "GRASP: a visualization tool for teaching security protocols," in the Tenth Colloquium for Information Systems Security Education, Adelphi, MD, 2006, pp. 1-7.

[22] C. Eckert, T. Clausius, B. Esslinger, J. Schneider, and H. Koy, "CrypTool," 2003.

[23] B. Esslinger, "The CrypTool Script: Cryptography, Mathematics, and More," 10 ed: Frankfurt am Main, Germany, 2010.

[24] M. A. Mayouf and Z. Shukur, "Animation of Natural Language Specifications of Authentication Protocol," Journal of Computer Science, vol. 4, pp. 503-508 2008.

[25] M. A. Mayouf and Z. Shukur, "Using Animation in Active Learning Tool to Detect Possible Attacks in Cryptographic Protocols," LNCS 5857, pp. 510-520, 2009.

[26] C. Kehoe, J. Stasko, and A. Taylor, "Rethinking the evaluation of algorithm animations as learning aids: an observational study," International Journal of Human Computer Studies, vol. 54, pp. 265-284, 2001.

[27] C. D. Hundhausen, S. A. Douglas, and A. T. Stasko, "A meta-study of algorithm visualization effectiveness," Journal of Visual Languages and Computing, vol. 13, pp. 259-290, 2002.

[28] J. Urquiza-Fuentes and J. A. VelAzquez-Iturbide, "A Survey of Successful Evaluations of Program Visualization and Algorithm Animation Systems," ACM Transactions on Computing Education, vol. 9, pp. 1-21, 2009.

[29] J. Pallant, SPSS Survival Manual: A step by step guide to data analysis using SPSS. Berkshire UK: McGraw-Hill Education, 2010.

[30] S. R. Hansen, N. H. Narayanan, and S. Douglas, "Helping Learners Visualize and Comprehend Algorithms Interactive Multimedia Electronic " Interactive Multimedia Electronic Journal of Computer-Enhanced Learning, vol. 2, 2000.

Authors

Mabroka Maeref: received her BSc degree in Computer Science from University of Sebha, Libya, MSc in Computer Science from Universiti Sains Malaysia, and PhD in Software Engineering from Universiti Kebangsaan Malaysia. Her interests span a wide range of topics in the area of Software Engineering, Networking, Computer Security, Visual Informatic and Computer Education. she is currently working as a lecturer at the departement of computer science, Faculty of Sciences in Sebha University of Libya.

Fatma Abdullah Alghali received a Ph.D. in Computer Science (Software Engineering) from University of AL-Neelain SUDAN 2006, Master of Computer Science from Warsaw University of Technology, Poland , 1997,BSc of Computer Science from Sebha University, Libya, 1991,Her research interest includes Software Engineering, Human Computer Interactive (HCI) , E-Learning, Cloud Computing, She is working as Assistant Professor. In Computer Science Department of Sebha University LIBYA.

Ahmed Patel received hisMSc and PhD degrees in Computer Science from Trinity College Dublin (TCD) in 1978 and 1984 respectively, specializing in the design, implementation and performance analysis of packet switched networks.. He is visiting professor at Kingston University in the UK. He is currently involved in the R&D of cybercrime investigations and forensic computing, intrusion detection & prevention systems, cloud computing autonomic computing, Web search engines, e-commerce and developing a framework and architecture of a comprehensive quality of service facility for networking protocols and advanced services.