RANDOM THESIS TITLE

A Thesis

Presented to the

Department of Information Systems

and Computer Science

Ateneo de Manila University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

by

Aldrich Ellis C. Asuncion

Brian Christopher T. Guadalupe

2019

ABSTRACT

This paper is a sample document that serves as a format and content guideline for undergraduate thesis submissions to the Department of Information Systems and Computer Science. In this section, the abstract, the group should be able to give the readers a clear and concise overview of their study. The section should contain the objectives of the thesis, the methods to be used, and when available, the results of the study, the conclusion, and the recommendations for further work, all based on the intended research objectives. A good abstract should be at most around 150–200 words, or half a page. It should also not contain any references, figures, or equations.

ACKNOWLEDGMENTS

We would like to thank Dr. Ma. Mercedes Rodrigo, Dr. Ma. Regina Estuar, and Dr. Proceso Fernandez, Jr. for initiating the creation of this thesis template for use of undergraduate thesis groups for years to come. We also extend our gratitude to Ms. Jessica Sugay for help invaluable help in automating many of the formatting of this template, especially in the creation of the custom styles, table of contents, list of figures, list of tables, and the bibliography.

This section, as the name suggests, is the place in your paper where you may acknowledge individuals or groups who, with their help or guidance, made your study feasible and ultimately a reality. Some of these people include your adviser, volunteers for your study, other professors who may have contributed to your study, and if applicable, any group or organization who provided support in any way for your research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION

In this section of the paper, you want to provide the general background and motivation of your study. This can be done defining some key definitions or ideas that govern your study, presenting your context, and narrowing it down with parameters that shall concretize your study. This chapter is divided into four parts: the Context of the Study, the Research Objective/s, the Research Questions, the Scope and Limitations, and finally, the Significance of the Study. Each will be described in greater detail in their respective sections. Appendix A summarizes major points for each of these sections and gives sample guide questions for your reference.

1.1 Context of Study

This subsection of the Introduction aims to discuss the fields related to your study. It is meant to benefit your readers, especially for those who have little or no background on the kind of work your study seeks to explore. You may also briefly discuss related work to help situate your reader. A sample context can be as follows: The use of agents within ITSs has been the subject of continuing research at the Ateneo de Manila University. A continuum of research work has been invested particularly in the design and development of emotionally intelligent agents for Aplusix. Early work in the area developed models of student emotion [2], [7] as well as preliminary designs for an agent [8]. The first three studies were synthesized into a working ECA [1], with an initial capability of detecting and responding to learner affect through the learners interaction with Aplusix. (p.2)

1.2 Research Questions

This subsection mainly presents your research objective/s in question form. An ideal research question must be open-ended, meaning that there is no clear answer that may be readily given to it. The recommended format for this section is that you provide a single overall question, followed by a series of sub-questions (enumerate them for better readability) that help you in answering your main question.

1. Research questions 1...
2. Research questions 2...
3. Research questions 3...

1.3 Research Objectives

With your context established, it is in this section where you will now describe what you intend to achieve by the end of the study. A possible way of presenting this subsection is to first introduce what problem/s you wish to address given the current context, and based on that/these, you present the objectives that would somehow address that/these problem/s. Other common things discussed may include a brief overview of your intended methodology.

1. Research objectives 1...

2. Research objectives 2...

3. Research objectives 3...

1.4 Scope and Limitations of the Study

In order for your study to be realistic, doable, and still produce a concise answer to your research questions within a particular period of time, this section provides you the opportunity to both cross-out extraneous variables, as well as set those aspects that must be controlled in your study. Some common limitation targets include the target audience for the experiment, the software to be used, portability and reusability of the software, the features it will have, and so on.

1.5 Significance of the Study

If the Research Objective answers the what of your study, this section aims to answer the why. Generally, you may address this significance in terms of its significance in the area of Computer Science and the community. However, other questions which you may also use to guide your significance are the following: Why is your study important? What will your study contribute to the field of Computer Science? How will your study benefit not only your intended audience, but the general public, especially our country?

CHAPTER II

REVIEW OF RELATED LITERATURE

Now that you have established what your study is, this section provides you the ability to look into your research area in order to find out what is the state-of-the-art regarding your topic of interest. By the end of this section, you should already have an idea of what has been done in relation to your work, what findings they had about their studies, and how your own study factors into what was observed (e.g. improvements based upon the studies recommendations, techniques that can be borrowed, delineating where previous work ends and where your study begins).

This is an equation:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Although it discusses a variety of literature, it is still important to maintain a general flow within your discussion. Make use of transitions and other literary means to connect the ideas of each discussed article. One way to do this is to first organize your articles into general topics of discussion. You may then introduce the flow of these topics in the first few paragraphs of this section, and use the topic outline you created as your guide in delivering, comparing and contrasting what ideas you may wish to present about the literature. You can also use the themes as your sub headings. Finally, summarize your literature review by briefly going through the key ideas of previous work, identify points for improvement, and state what your study can do to contribute in addressing those points.

Last but not the least, do not forget to put proper citations to the ideas you will present. More often than not, whatever idea you state here came from another source, so ensure that you acknowledge the article/book/other reference you may have lifted it from. In order to guide you in writing, as well as to summarize the points mentioned above, here are some questions that may help your structure your discussion:

1. What previous works are closely connected with your own study? Who initiated these studies?

2. What objectives did these studies have? If they presented any research questions, what were these and how similar or different are they from your own set of questions? Describe the methods used in these studies. If there are test subjects, what is the general profile of their subjects?

3. What instruments did they use to acquire and measure their data?

4. What were the findings gathered from the studies?

5. What issues, if any (e.g. flaws or gaps in the methodology), were encoun-

tered during the implementation of the study? In what way did the researchers attempt to address these issues? Were they successful in resolving these issues? Why or why not?

6. What conclusions did these studies have? What recommendations did they present, and which of these recommendations may be addressed through your study?

7. What other improvements could be done that was not mentioned in the study? How will your study incorporate these improvements?

8. In what way is your study different or novel given these previous studies? Where do their studies end, and where will yours begin?

Below is a sample entry from a literature review. You may use this as basis for your own work.

2.1 Motivation and ECAs

In applying motivational concepts to ECAs, some previous work includes studies by Rebolledo-Mendez et al. [9] and Graesser et al [4, 5]. Rebolledo-Mendez et al. [9] investigated the effect of a motivational version of Ecolab, an ITS for teaching primary school children the topic of Ecology, particularly about food chains and food webs. In implementing the motivational extension, they modeled three motivational traits identified as key in the learning context. These are effort, confidence, and independence from the tutor [9]. The motivational on-screen character, which they named as Paul, was designed to provide feedback before and after each activity. Each post-activity feedback was based on the motivational model of the learner, and using this, Paul encourages the learner: to exert more effort, to be more independent, or to become more confident [9].

The results of the study showed that through modeling motivation and adjusting motivational reaction, the de-motivated, low, and average students were able to significantly increase their post-test scores. It also, however, showed that highly motivated and high ability students had no increase in test scores. The researchers noted that this could be due to the ceiling effect. Nevertheless, it was highlighted that the effects on learning by these motivating techniques were different, depending on the students ability and motivation. An example would be adjusting spoken feedback considering the learners motivational state as an important influence at post-activity time [9]. There were, however, some limitations to the study. One of these was that the results were derived from a very small sample. Another limitation they indicated was that adapting feedback and characters reactions, in conjunction with a quiz, constitute only a first step in the study of motivating techniques in ITSs; thus, general guidelines could be used in order to improve student motivation [9]. On the other hand, Graesser et al. [4] developed a computer tutor called AutoTutor, which simulated the discourse patterns and pedagogical strategies of a typical human tutor. It was designed for college students in introductory computer literacy courses, who learn the fundamentals of hardware, operating systems, and the Internet [4].

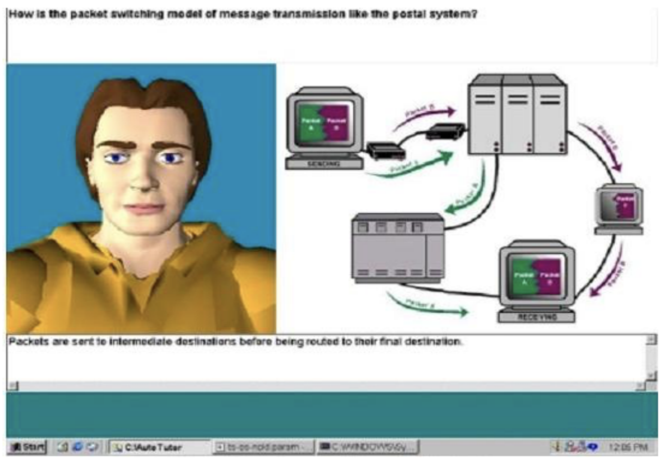

Figure 2.1: The AutoTutor Interface.

AutoTutor works by initiating a conversation with the student. It appears as a talking head that acts as a dialogue partner with the learner, who contributes to the conversation via input from the keyboard. One thing notable about the tutor is that it encourages the learner to articulate answers that are lengthy and require deep reasoning examples of which include answers to why, how, and what-if questions. There is a multi-turn dialogue involved between AutoTutor and the student, encouraging the student to construct the knowledge and discover what he or she has mastered, rather than bombarding the student with the information to master [4]. Results of the study show that this strategy of AutoTutor was able to influence learning and mastery of students. Comparing students who used AutoTutor to those who only reread the topic and to the control group who did not reread, AutoTutor was able to help students answer more questions which were used in an actual computer literacy course, garnering a greater score than the two other groups [4]. In terms of the conversational smoothness and pedagogical quality of dialogue, an experiment was done where students were asked to point out which dialogue moves were generated by human tutors and which ones were by AutoTutor. Results show that the students were unable to discriminate the dialogue moves that were computer-generated compared to those from human tutors. In reality, half of the dialogue was by human tutors and the other half by AutoTutor. This proved the ability of AutoTutor to accurately simulate a human tutor [4]. In a related study, Graesser et al. [5] was able to determine that during interactions with the AutoTutor, confusion was a great predictor of post-test scores. The study showed that when the learner is confused the learner experiences cognitive disequilibrium and thinking. It is presumed that the other frequent emotions such as frustration, bored and flow play a more prominent role in other learning environments and population of learners. It is therefore suggested that further research be conducted on these frequent emotions to discover different strategies and dialogues that will promote both learning gains and more engagement for the students [5].

2.2 New Sample Subsection

This is added in between existing subsections.

2.3 Sample Subsection

Blah blah blah blah!

2.4 Sample Sample Subsection New

This is added after the last existing subsection. Updated the TOC, it works.

CHAPTER III

METHODOLOGY

After introducing your topic of choice, discussing and relating previous work with your own, and presenting the underlying concepts that your study will be working with, this section will enable you to go into fine detail into how you will go about your study. Essentially, whatever data you need to gather, as well as how you will intend to gather them, should be presented here. In order to check whether or not your methodology is sound, two main questions should be answered:

1. Is your methodology replicable?
2. Is your methodology realistic and time-bound?

3.1 Methodology as Replicable

A replicable methodology basically means that anyone who reads your methodology and intends to recreate your study to the letter must be able to obtain a similar, if not, exactly the same set of results. It is important, therefore, that you be as specific as you can when describing your methods, such as properly delineating your studys independent, dependent, and control variables. Much like in the literature review and framework, it is good practice to organize your methodology into subsections for easier readability. Of course, apart from generating data given these variables, included in making the methodology replicable is providing the users an effective and appropriate means to collect data for analysis later on. This assumes, of course, that the data you intend to collect is actually measurable, whether it be quantitative (numerical) or qualitative (descriptive).

3.2 Methodology as Realistic and Time-Bound

On the other hand, a realistic and time-bound methodology takes into consideration the context of the researcher. Although a high-level of competency is expected from a graduating CS major, one must also ensure that the proposed studys level of difficulty is aligned with what limited resources is available, especially time. In fact, given that the trend is that you will undergo actual implementation only after being able to defend your proposal during the first semester, the study should be accomplishable at the most within only a semester. It is therefore imperative in the methodology, especially in its initial presentation during the defense, that the timetable for the study is thoroughly laid out, with workable time frames and specific dates for deliverables.

3.3 Summary and Additional Guide Questions

The methodology, in summary, is your detailed explanation of how you intend to go about implementing your study.

CHAPTER IV

RESULTS AND DISCUSSION

After implementing your methodology and gathering all pertinent data, in this section, you will now present the gathered data to your reader. By the end of this section, your reader should have an idea of what exactlty happened during the experiment. A good way to organize your results is to group them is to present them in the same order which your methodology was presented. For instance, if your methodology included the analysis of user logs, the implementation of an application, and the testing of this application, your results should flow in the same way. In addition, more often than not, you will be presenting a large volume of data, so utilize figures and tables whenever appropriate. Table 5.1 below presents one way of how to go about presenting your data. Note the table caption and headers, as mentioned in our framework.

There are, however, some additional notes that must be clarified. First, given that you will be gathering a huge volume of data, you must be able to classify which of these were critical in determining the outcome of your study, and which ones need not be presented. The critical data must be presented in this section, while the minor ones may be placed in the Appendices of your paper, which will be described later in this template.

Table 4.1: Preliminary Test Result, organized by Problem Type

Problem Type	Average Steps	Standard Deviation (Steps)	Average Duration (s)	Standard Deviation (Duration)	Dominant Affective State
A1	14	2.30	23.04	3.50	CONF
A2	2	5.36	32.10	2.01	FLOW
A3	31	1.01	28.55	4.03	FLOW
B1	24	4.40	45.30	3.30	BOR
B2	33	2.12	20.56	2.21	FLOW
B3	36	1.05	LOSE	1.15	CONF
C1	22	1.33	LOSE	1.40	FLOW
C2	23	3.03	LOSE	1.30	FLOW
D1	30	1.79	LOSE	1.45	FLOW
D2	15	1.30	LOSE	1.05	FLOW

Another clarification to be noted is that the presentation of results in this section must be objective, or 'as-is'. This means that you must describe your results in a way understandable to your reader without putting any form of interpretation. In effect, this sections intent is to provide answers to "what happened" questions, not "what does it mean" questions. The interpretation of results is the subject of a later section.

Finally, because this is a presentation of what happened in the past, all tenses used in this section must be in the past form, be it active or passive. This will also be true for the preceeding sections after the studys implementation, especially when stating the methodology.

CHAPTER V

CONCLUSIONS

Upon presenting your results, the conclusion is where you will now tie up these results with the original intent of the study, as indicated by the research questions given in the Introduction. It is in this section where you will also discuss any difficulties or issues encountered during the study, as well as your recommended method for addressing these problems.

The general way to organize your conclusion is to present each research sub-question as a subsection, and thoroughly answer each of them by interpreting your results with respect to the question. With these answered, you may then tie up all of your findings in each subsection to answer your main research question, providing any needed additional information or explanation. Last on the list would be your unsolved issues and difficulties, presenting them as avenues to motivate continued work on your chosen topic.

BIBLIOGRAPHY

[1] El-Samie, F. E. A., Ahmed, H. E. H., Elashry, I. F., Shahieen, M. H., Faragallah, O. S., El-Rabaie, E.-S. M., and Alshebeili, S. A. Homomorphic Image Encryption. In *Image Encryption: A Communication Perspective*. CRC Press, 2014, pp. 43–55.

[2] Fontaine, C., and Galand, F. A Survey of Homomorphic Encryption for Nonspecialists. *EURASIP Journal on Information Security 2007* (2007), 1–10.

[3] Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 2009), STOC '09, ACM Press, pp. 169–178.

[4] Goldwasser, S., and Micali, S. Probabilistic encryption. *Journal of Computer and System Sciences 28*, 2 (Apr. 1984), 270–299.

[5] Gonzalez, R. C., and Woods, R. E. *Digital Image Processing*, 3rd ed. Prentice Hall, Upper Saddle River, N.J, 2008.

[6] Iyer, S. C., Sedamkar, R., and Gupta, S. A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach. *Procedia Computer Science 79* (2016), 293–298.

[7] Khoirom, M. S., Laiphrakpam, D. S., and Themrichon, T. Cryptanalysis of multimedia encryption using elliptic curve cryptography. *Optik 168* (Apr. 2018), 370–375.

[8] Koblitz, N., and Menezes, A. J. A Survey of Public-Key Cryptosystems. *SIAM Review 46*, 4 (Jan. 2004), 599–634.

[9] Li, L., Abd El-Latif, A. A., and Niu, X. Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. *Signal Processing 92*, 4 (Apr. 2012), 1069–1078.

[10] Lian, S., and Chen, X. On the design of partial encryption scheme for multimedia content. *Mathematical and Computer Modelling 57*, 11-12 (June 2013), 2613–2624.

[11] Martins, P., Sousa, L., and Mariano, A. A Survey on Fully Homomorphic Encryption: An Engineering Perspective. *ACM Computing Surveys 50*, 6 (Dec. 2017), 1–33.

[12] SEN, J. Homomorphic Encryption: Theory and Application. In *Theory and Practice of Cryptography and Network Security Protocols and Technologies*, J. Sen, Ed. InTech, July 2013.

[13] SHORTELL, T., AND SHOKOUFANDEH, A. Secure Fast Fourier Transform using Fully Homomorphic Encryption. *arXiv:1611.08769 [cs]* (Nov. 2016). arXiv: 1611.08769.

[14] SINGH, L. D., AND SINGH, K. M. Image Encryption using Elliptic Curve Cryptography. *Procedia Computer Science 54* (2015), 472–481.

[15] TILBORG, H. C. A., Ed. *Encyclopedia of Cryptography and Security*. Springer US, 2005.

[16] UPMANYU, M., NAMBOODIRI, A. M., SRINATHAN, K., AND JAWAHAR, C. V. Efficient privacy preserving video surveillance. In *2009 IEEE 12th International Conference on Computer Vision* (Sept. 2009), pp. 1639–1646.

[17] YI, X., PAULET, R., AND BERTINO, E. *Homomorphic Encryption and Applications*. SpringerBriefs in Computer Science. Springer International Publishing, Cham, 2014.

[18] Ziad, M. T. I., Alanwar, A., Alzantot, M., and Srivastava, M. CryptoImg: Privacy Preserving Processing Over Encrypted Images. *arXiv:1609.00881 [cs]* (Sept. 2016). arXiv: 1609.00881.