IMPLEMENTATION AND ANALYSIS OF HOMOMORPHIC IMAGE ENCRYPTION AND IMAGE MANIPULATION

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

1.1 Context of the Study

Digital data privacy and security is a growing concern in various fields, such as cloud computing [25], health information systems [17], and video surveillance [32]. To meet these needs, various cryptosystems have been developed. A cryptosystem is a system which operates on plaintexts, ciphertexts and keys. a cryptosystem also has an encryption algorithm, which maps a plaintext to a ciphertext, and a decryption algorithm, which maps a ciphertext to a plaintext, given an appropiate key [4]. The encryption and decryption algorithms are chosen such that the plaintext cannot easily be recovered from the ciphertext without knowledge of the key. This allows data to be securely transmitted over an insecure channel: and thus much research has been done on the development and application of various cryptosystems.

One such particular application of cryptography is image encryption. While cryptosystems used to encrypt digital data in general, such as the Advanced Encryption Standard (AES) or elliptic curve cryptography, can also be used to encrypt images [16, 29] other algorithms created specifically for image encryption have also been developed [23].

However, research has also considered a type of cryptosystem, homomorphic cryptosystems, where in addition to allowing the secure transmission of data, it is also possible to perform computations with encrypted data, the most basic of which being addition and multiplication. Numerous homomorphic cryptosystems exist, which allow for data to be manipulated without compromising data privacy [8, 27]. In homomorphic image encryption, there is additional interest in being able to perform image manipulation operations on the encrypted data such as image adjustment, filtering, and morphological/feature extraction operations [36, 11].

1.2 Research Objectives

A paper published in 2009 by Ziad, et. al. presents *CryptoImg*, a library for the Open Source Computer Vision Library (OpenCV) [6] which implements various homomorphic encryption and image processing routines using the Paillier homomorphic cryptosystem [36]. While *CryptoImg* demonstrates that various image manipulation operations are possible in a homomorphic system, we believe this study can be extended by considering other known homomorphic encryption schemes, such as an elliptic curve and ElGamal based cryptosystem presented by Li, et. al. [20], and the fully homomorphic encryption scheme proposed by Smart and Vercauteren [30]. Our study aims to provide an objective comparision of various homomorphic cryptosystems currently in the literature, as they would be used in encrypted image manipulation. Furthermore, one of the main problems in homomorphic encryption is the practicality of homomorphic encryption schemes. Homomorphic cryptosystems are known to be slower compared to other cryptosystems [27]. Taking the above into account, in this study, we wish to

1. Compare the applicability of known homomorphic encryption schemes to common image processsing operations, in other words, determine which schemes permit more image processing operations;

2. Compare the security of common image processing operations under known homomorphic encryption schemes, using established statistical methods in image encryption;

3. Compare the efficiency of common image processsing operations under known homomorphic encryption schemes;

4. Create a library for OpenCV to allow for convenient use and comparison of these homomorphic encryption schemes.

1.3 Research Questions

In this study, we ask the following main research question: What is the best method for image data to be encrypted and manipulated for practical applications?

To answer this question, we will consider the following sub-questions in our research:

1. Which homomorphic image encryption algorithms are the most applicable for image processing operations?
2. Which homomorphic image encryption algorithms are the most efficient in terms of time when applying image manipulation operations?
3. Which homomorphic image encryption algorithms are the most secure under differential and entropy attacks?

1.4 Scope and Limitations of the Study

Our study will be limited in terms of the cryptosystems to be tested, the image processing operations we will implement, and the statistical tests we will use to gauge the security of the cryptosystems. Below is a listing of the scope of the study.

We will implement and test the following algorithms:

1. A modified version of the Paillier cryptosystem [24] which supports floating-point operations, used in *CryptoImg* [36].

2. An elliptic curve and ElGamal based cryptosystem for homomorphic encryption presented by Li, et. al. [20].

3. A fully homomorphic encryption scheme proposed by Smart and Vercauteren [30], which is an improvement on the original lattice-based cryptosystem presented by Gentry [9].

We will implement and test the following categories of image manipulation operations:

1. Image adjustment

2. Spatial filters/morphological operations

We will adopt the benchmark for evaluating the performance and security of image encryption schemes presented by Ahmed, et. al [2]. The presented benchmark reflects many tests used in other literature [1, 34].

1. Tests for preservation of image quality after encryption and decryption.

   (a) Mean Squared Error (MSE)

   (b) Peak Signal to Noise Ratio (PSNR)

   (c) Structural Similarity Index (SSIM)

2. Tests for cryptographic security

    (a) Information entropy analysis

    (b) Correlation coefficient analysis

    (c) Differential analysis (number of pixel change rate (NPCR), universal average change intensity (UACI))

A detailed overview of the above will be provided in the methodology. Both greyscale and color images will be used in the study.

Our library for OpenCV will be implemented in the C++ programming language.

The study will only consider the operation of the stated algorithms in a single computer. Client-server models for secure data storage and operation will not be considered.

1.5 Significance of the Study

This study aims to directly address one of the current problems in the research of homomorphic cryptosystems: the practicality of homomorphic encryption [27]. The literature shows existing homomorphic cryptosystems and how they support primitive operations (usually addition and multiplicaiton) on encrypted data, however, for homomorphic cryptosystems to be usable for practical image processing applications, support for more complicated operations such as image convolution must be demonstrated as well. While implementations of homomorphic encryption algorithms exist [36, 13], our study targets algorithms for which statistical tests were not performed for image processing operations.

By developing a library allowing for the use and comparison of various homomorphic encryption algorithms, we wish to contribute to existing models for the secure transmission and modification of image data. Examples include applications in cloud storage [25] and video surveillance [32]. This allows service providers to perform image manipulation for clients without compromising data privacy.

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?

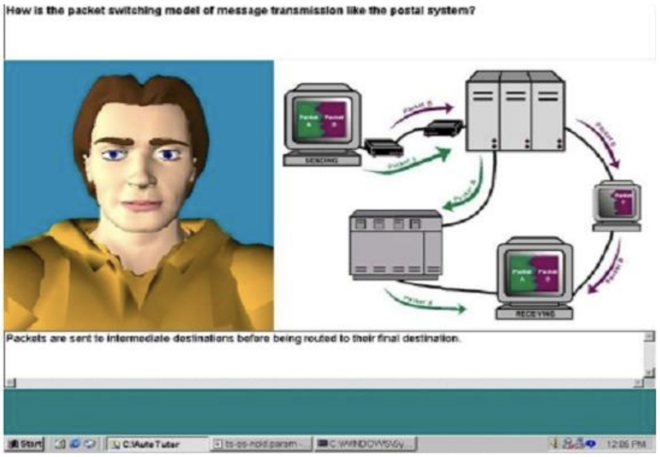
8. In what way is your study different or novel given these previous studies? Where do their studies end, and where will yours begin?

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].


How is the packet switching model of message transmission like the postal system?

Packets are sent to intermediate destinations before being routed to their final destination.

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

The study consists of two parts: first, the implementation of the three homomorphic encryption schemes and image processing operations under each scheme as an OpenCV library. The second part of the study consists of assessing the robustness and security of image operations under each encryption scheme using benchmarks in [2].

3.1 Implementation of the OpenCV Library

The current version of the OpenCV library (3.4.1) will be forked from the open-source GitHub repository at https://github.com/opencv [6].

Three homomorphic encryption schemes will be implemented, those presented by Ziad, et al. [36], Li, et al. [20] and Smart and Vercauteren [30]. The encryption and decryption methods will be implemented in C++.

Aside from implementing the homomorphic encryption and decryption algorithms, we will also implement library functions for the following image processing functions, as they are defined in [11]. We will also take note of whether or not a candidate operation is impossible to perform under a given cryptosystem. We let $R(x, y)$ denote the intensity at coordinate (x, y) in the source image, and $S(x, y)$ denote the intensity at coordinate (x, y) in the resulting image. We further suppose that the intensity values of pixels are in the range $[0, L - 1]$.

Intensity transformations. Transformations on the intensities of each of the pixels on an image. The following definitions hold for all x, y.

1. Image negation: $S(x, y) = L - 1 - R(x, y)$.
2. Log transformation: $S(x, y) = c \log(1 + R(x, y))$, $c \geq 0$.
3. Power-law transformation: $S(x, y) = c[R(x, y)]^\gamma$, $c > 0, \gamma > 0$.

Spatial filters. Filters implemented by performing a convolution between an $M \times N$ source image and an $m \times n$ filter matrix. Let W be a filter matrix. Then the corresponding spatial filter is given by

$$S(x, y) = \sum_{s=1}^{m} \sum_{t=1}^{n} W(s, t) R(x + s, y + t). \tag{3.1}$$

Morphological operations such as erosion and dilation can be achieved using convolution as well.

3.2 Assessment of Homomorphic Encryption Schemes

We will first obtain standard test images from [12]. Both greyscale and color images will be used.

For each plaintext image (PT), we will consider each image operation listed above and generate three images: a plaintext domain transformation

(PDT), a ciphertext image (CT), and an encrypted domain transformation (EDT). The cipherThe PDT will be generated by running the image operation on the original image. The CT will be generated by encrypting the image, then applying the operation, and the EDT will be generated by decrypting the CT. The four images (PT, PDT, CT, CDT) will then be compared using various benchmarks to evaluate the quality and security of each homomorphic encryption scheme.

Lab computers in Faura Hall, Ateneo de Manila University will be used to perform the computations, and processing time will be tracked using C++ timer functions. The processing time for all cases will be recorded.

3.2.1 Evaluating Image Quality

The benchmarks to be used in the study, adopted from [2, 1, 34] are listed below. We let X_i denote a value in an image X, where $1 \leq i \leq N$. We first perform three tests to ascertain the preservation of image quality after encryption and decryption: MSE, PSNR, and SSIM.

Mean Squared Error (MSE). The MSE is defined in [2] as

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (CDT_i - PDT_i)^2. \tag{3.2}$$

The MSE provides a measure of how much data is recovered if an image operation is applied on the encrypted image, which is then decrypted. Lower values of MSE indicate higher preservation of image quality [2, 1].

Peak Signal to Noise Ratio (PSNR). According to Ahmed, et al. [2], PSNR is "an estimator for human visual perception of reconstruction quality" which is based on It has been used to ascertain image quality in various studies and is a known meetric for image and video quality [32, 16, 3]. Although it may produce results which do not correlate with human visual perception [14, 2], it is a valid indicator of image quality when media containing the same visual content is compared [14]. PSNR is defined by

$$PSNR = 10\log_{10}\left(\frac{L^2}{MSE}\right) \tag{3.3}$$

where L is the maximum pixel intensity value of an image. Despite the known limitations of PSNR, since we are going to compare the effect of each encryption scheme on recovered image quality, given a fixed library of images, it is a valid measure of image quality for the study. A higher PSNR indicates higher image quality preservation.

Structural Similarity Index (SSIM). The SSIM for two random variables X and Y is defined in [2, 3] as

$$SSIM(X, Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_{XY} + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\mu_X^2 + \mu_Y^2 + c_2)} \tag{3.4}$$

where

- μ_X, μ_Y are the averages of X and Y, respectively;
- σ_X, σ_Y are the variances of X and Y, respectively;

- σ_{XY} is the covariance of X and Y;
- $c_1 = (k_1L)^2, c_2 = (k_2L)^2$ are two variables used to stabilize the measure when $\mu_X^2 + \mu_Y^2$ is close to zero [3];
- L is the the maximum pixel intensity value of an image;
- $k_1 = 0.01, k_2 = 0.03$ by default, given in [2].

The SSIM is applied to the luminance value of two images to gauge structural similarity between neighboring pixels. For the study, we will compute $SSIM(PDT, CDT)$ for every image operation, under each homomorphic cryptosystem. Higher values of SSIM indicate higher structural similarity, and an SSIM of 1 indicates that the two images are identical[2].

3.2.2 Evaluating Cryptographic Security

After performing tests to evaluate image quality, we then perform tests for cryptographic security, as enumerated in [2]: entropy analysis, correlation coefficient analysis (CC), NPCR and UACI.

Information entropy analysis. In information theory, the entropy function $H(X)$ is defined in [5] as

$$H(X) = -\sum_{a:p_X(a)>0} p_X(a) \log_2 p_X(a) \tag{3.5}$$

where $p_X(a)$ denotes the probability that the random variable X takes on the value a. In the analysis of image encryption, $H(X)$ is computed for the values of the ciphertext pixels. To ensure security against entropy attacks, $H(X)$ must be as close as possible to $\log_2 N$, where N is the number of possible pixel values [2].

We will compute $H(CDT)$ for every image operation, under each homomorphic cryptosystem, and compare the effects of each image operation on the entropy of the encrypted image. Ideally, performing image operations on encrypted images should still maintain a high level of entropy.

Correlation coefficient analysis (CC). Images generally have a high degree of similarity between adjacent pixels. This correlation must be hidden in the encrypted image, even after performing image operations. The correlation coefficient of an image can be computed between adjacent pixels either vertically, horizontal, or diagonally, and is defined in [2] by:

$$CC(X,Y) = \frac{\sigma_{X,Y}}{\sqrt{\sigma_X} \times \sqrt{\sigma_Y}} \tag{3.6}$$

where

- σ_X, σ_Y are the variances of X and Y, respectively;
- σ_{XY} is the covariance of X and Y.

For every CDT image, we will compute for the correlation coefficient (for vertical, horizontal and diagonal correlation) for every image operation, under each homomorphic cryptosystem.

NPCR and UACI. The Number of Pixel Change Rate (NPCR) measures the number of pixels which are changed between the a plaintext and a ciphertext to quantify the amount of dispersion which occurs during encryption.

On the other hand, the Universal Average Change Intensity (UACI) measures the average difference in pixel intensity between two images.

The NPCR and UACI between two images X and Y, each containing N pixels indexed from 1 to N is defined in [34] as

$$NPCR(X,Y) = \frac{1}{N}\sum_{i=1}^{N} D(X_i, Y_i) \times 100\% \tag{3.7}$$

$$UACI(X,Y) = \frac{1}{L_{max} \times N}\sum_{i=1}^{N} |L(X_i) - L(Y_i)| \times 100\% \tag{3.8}$$

where

- X_i and Y_i are the ith pixels of X and Y, respectively;
- D is a difference function between pixels A and B defined by

$$D(A,B) = \begin{cases} 0 & \text{if } A = B, \\ 1 & \text{if } A \neq B; \end{cases} \tag{3.9}$$

- L_{max} is the maximum intensity of a pixel;
- $L(X_i)$ and $L(Y_i)$ are the intensities of pixels X_i and Y_i, respectively.

We will calculate $NPCR(PDT, CDT)$ and $UACI(PDT, CDT)$ for every image operation, under each homomorphic cryptosystem. A high NPCR and UACI are desired to ensure high dispersion and security against differential attacks [2]. Critical values for NPCR and UACI for given image sizes and bit depths are given in [34].

3.3 Summary

We now recap the research questions and the corresponding methodology.

- **Applicablity of homomorphic encryption algorithms for the use of image processing operations on encrypted data?** This will be addressed by the implementation of OpenCV library, and the evaluation of image quality (MSE, PSNR, SSIM).
- **Time efficiency in applying image manipulation operations.** This will be addressed by the implementation of OpenCV library, and the comparison of recorded processing time for image processing operations.
- **Security under differential and entropy attacks.** This will be addressed by the evaluation of security benchmarks for image encryption schemes (entropy analysis, correlation coefficient analysis, NPCR, UACI).

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] AHMAD, J., AND AHMED, F. Efficiency Analysis and Security Evaluation of Image Encryption Schemes. *International Journal of Video & Image Processing and Network Security 12*, 04 (Aug. 2012), 18–31.

[2] AHMED, N., SHAHZAD ASIF, H. M., AND SALEEM, G. A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes. *International Journal of Computer Network and Information Security 8*, 12 (Dec. 2016), 28–29.

[3] AKRAMULLAH, S. Video Quality Metrics. In *Digital Video Concepts, Methods, and Metrics*. Apress, Berkeley, CA, 2014, pp. 101–160.

[4] BAUER, F. L. Cryptosystem. In *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg, Ed. Springer US, 2005, pp. 119–119.

[5] BAUER, F. L. Information Theory. In *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg, Ed. Springer US, 2005, pp. 289–290.

[6] BRADSKI, G. The OpenCV Library. *Dr. Dobb's Journal of Software Tools* (2000).

[7] 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.

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

[9] 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.

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

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

[12] Gonzalez, R. C., Woods, R. E., and Eddins, S. Image Databases - Image Processing Place.

[13] Halevi, S., and Shoup, V. Algorithms in HElib. In *Advances in Cryptology CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds., vol. 8616. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 554–571.

[14] Huynh-Thu, Q., and Ghanbari, M. The accuracy of PSNR in predicting video quality for different video scenes and frame rates. *Telecommunication Systems 49*, 1 (Jan. 2012), 35–48.

[15] 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.

[16] Jain, Y., Bansal, R., Sharma, G., Kumar, B., and Gupta, S. Image Encryption Schemes: A Complete Survey. *International Journal of Signal Processing, Image Processing and Pattern Recognition 9*, 7 (July 2016), 157–192.

[17] Kester, Q.-A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., and Quaynor, N. N. A Cryptographic Technique for Security of Medical Images in Health Information Systems. *Procedia Computer Science 58* (2015), 538–543.

[18] KHOIROM, M. S., LAIPHRAKPAM, D. S., AND THEMRICHON, T. Cryptanalysis of multimedia encryption using elliptic curve cryptography. *Optik 168* (Apr. 2018), 370–375.

[19] KOBLITZ, N., AND MENEZES, A. J. A Survey of Public-Key Cryptosystems. *SIAM Review 46*, 4 (Jan. 2004), 599–634.

[20] 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.

[21] 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.

[22] 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.

[23] MURUGAN, C. A., AND KARTHIGAIKUMAR, P. Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms. *Mobile Networks and Applications* (May 2018).

[24] PAILLIER, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology EUROCRYPT 99*, J. Stern, Ed., vol. 1592. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999, pp. 223–238.

[25] POTEY, M. M., DHOTE, C., AND SHARMA, D. H. Homomorphic Encryption for Security of Cloud Data. *Procedia Computer Science 79* (2016), 175–181.

[26] RIVEST, R. L., SHAMIR, A., AND ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM 21*, 2 (Feb. 1978), 120–126.

[27] 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.

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

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

[30] SMART, N. P., AND VERCAUTEREN, F. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In *Public Key Cryptography PKC 2010*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, P. Q. Nguyen, and D. Pointcheval, Eds., vol. 6056. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 420–443.

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

[32] UPMANYU, M., NAMBOODIRI, A. M., SRINATHAN, K., AND JAWAHAR, C. V. Efficient privacy preserving video surveillance. IEEE, pp. 1639–1646.

[33] 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.

[34] WU, Y., NOONAN, J., AND AGAIAN, S. NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JS* (Apr. 2011), 31–38.

[35] Yi, X., Paulet, R., and Bertino, E. *Homomorphic Encryption and Applications*. SpringerBriefs in Computer Science. Springer International Publishing, Cham, 2014.

[36] 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.