UNIVERSITY OF MIAMI

BIOMETRICS FOR CYBERSECURITY AND UNCONSTRAINED ENVIRONMENTS

By

Mohammad Haghighat

A DISSERTATION

Submitted to the Faculty
of the University of Miami
in partial fulfillment of the requirements for
the degree of Doctor of Philosophy

Coral Gables, Florida

August 2016

UNIVERSITY OF MIAMI

A dissertation submitted in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

BIOMETRICS FOR CYBERSECURITY AND UNCONSTRAINED ENVIRONMENTS

Mohammad Haghighat

Approved:

Mohamed Abdel-Mottaleb, Ph.D.
Professor of Electrical and
Computer Engineering

Saman Zonouz, Ph.D.
Assistant Professor of Electrical and
Computer Engineering
Rutgers University

Shahriar Negahdaripour, Ph.D.
Professor of Electrical and
Computer Engineering

Jie Xu, Ph.D.
Assistant Professor of Electrical and
Computer Engineering

Anil K. Jain, Ph.D.
Distinguished Professor of
Computer Science and Engineering
Michigan State University

Guillermo Prado, Ph.D.
Dean of the Graduate School

HAGHIGHAT, MOHAMMAD (Ph.D., Electrical and Computer Engineering)

Biometrics for Cybersecurity and Unconstrained Environments (August 2016)

Abstract of a dissertation at the University of Miami.

Dissertation supervised by Professor Mohamed Abdel-Mottaleb.
No. of pages in text. (9)

Abstract goes here ...

to my whatever

Acknowledgements

I would like to thank my advisor Dr. Mohamed Abdel-Mottaleb and my co-advisor Dr. Saman Zonouz who supported me in the past few years through the research and completion of my degree. I believe their personality and technical capability was an indispensable factor for me to finish this endeavor.

Mohammad Haghighat

University of Miami

August 2016

Table of Contents

LIST OF FIGURES **vi**

LIST OF TABLES **vii**

1 INTRODUCTION **1**

2 CHAPTER TWO TITLE **2**

2.1 Equations 3

2.2 Section Title 4

2.2.1 SubSection Title 4

2.2.1.1 SubSubSection Title 4

3 CHAPTER THREE TITLE **5**

4 CONCLUSION **6**

APPENDIX **7**

BIBLIOGRAPHY **9**

List of Figures

2.1 This is where the caption of the figure goes. 3

List of Tables

2.1 This is where the caption of the table goes. 4

2.2 Rank-1 recognition rates for multimodal fusion of face, ear and profile face biometrics in WVU database. 4

CHAPTER 1

Introduction

Introduction goes here...

CHAPTER 2

Chapter Two Title

This is just a sample writing to show how to insert figures, tables, equations, and citations.

Each chapter can be divided into several sections, sub-sections, and sub-sub-sections as below. Each section or sub-section is identified by a *label* that is unique for that specific part. If you would like to refer to one of these parts you just insert the label title into the *ref* like Section 2.2. In LaTeX, you can easily reference almost anything that is numbered (sections, figures, tables, formulas), and LaTeX will take care of numbering, updating it whenever necessary. The commands to be used do not depend on what you are referencing. As an example, Fig. 2.1 shows a sample figure and Table 2.1 shows a sample table.

Citing a given document is very easy. Go to the point where you want the citation to appear, and use the [1], where the term between the curly brackets is that of the bibitem you wish to cite. The list of the bibitems must be included in the *references.bib* file. You can also refer to more than one documents in one location [2–4].

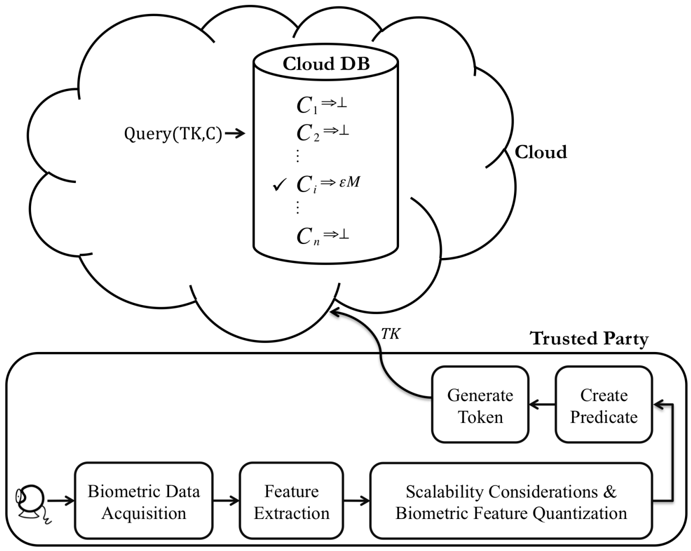

Figure 2.1: This is where the caption of the figure goes.

2.1 Equations

Section 2.1 is just an example to show how to insert inline and numbered equations.

The inline equations has to be inserted between two dollar signs. Some examples are: X', or Y', or $S'_{xy_{(r\times r)}}$.

The numbered equations, on the other hand, need to be placed in an equation environment beginning and ending as below:

$$(U\Sigma^{-1/2})^T\, S'_{xy}\,(V\Sigma^{-1/2}) = I\;, \tag{2.1}$$

which is numbered as Eq. 2.1.

Eq. 2.2 is an example of a multi-line equation:

$$\begin{aligned} G(x,y) = \frac{f^2}{\pi\gamma\eta} exp\left(-\frac{x'^2+\gamma^2 y'^2}{2\sigma^2}\right) exp(j2\pi f x' + \phi) \\ x' = \quad xcos\theta + ysin\theta \\ y' = -xsin\theta + ycos\theta \end{aligned} \tag{2.2}$$

Table 2.1: This is where the caption of the table goes.

Method	Run Time (in milliseconds)
Serial + PCA + KNN	19
Serial + LDA + KNN	24
Parallel + PCA + KNN	39
Parallel + LDA + KNN	42
PCA + CCA + KNN	19
LDA + CCA + KNN	21
JSRC	8406
SMDL	7882
DCA + KNN	19

2.2 Section Title

This is an example to show how to insert sections in your chapter.

2.2.1 SubSection Title

This is an example of a sub-section. Table 2.1 is just an example to show how to insert tables.

2.2.1.1 SubSubSection Title

This is an example of a sub-sub-section, and another Table 2.2.

Table 2.2: Rank-1 recognition rates for multimodal fusion of face, ear and profile face biometrics in WVU database.

Modality / Method	Face+Ear	Ear+Profile	Face+Ear +Profile
Serial + PCA + KNN	89.14 ± 1.15	89.46 ± 1.13	92.28 ± 1.11
Serial + LDA + KNN	94.23 ± 1.02	95.14 ± 1.20	95.14 ± 1.04
Parallel + PCA + KNN	90.71 ± 2.05	90.61 ± 1.86	-
Parallel + LDA + KNN	93.38 ± 1.66	93.13 ± 1.67	-
PCA + CCA/MCCA + KNN	94.10 ± 0.87	94.34 ± 0.57	97.74 ± 0.54
LDA + CCA/MCCA + KNN	94.44 ± 0.88	94.89 ± 0.54	97.86 ± 0.49
JSRC	96.20 ± 0.52	97.74 ± 0.42	98.74 ± 0.32
SMDL	97.24 ± 0.48	97.97 ± 0.42	99.20 ± 0.24
DCA/MDCA + KNN	98.56 ± 0.15	99.38 ± 0.08	99.85 ± 0.03

CHAPTER 3

Chapter Three Title

Chapter three goes here ...

CHAPTER 4

Conclusion

Conclusion goes here ...

APPENDIX

Proof of the Security of the CloudID

We review the proof of the security of CloudID's searchable encryption scheme presented in [1]. Let's define a security game in which an adversary is given a number of tokens and is required to distinguish two encrypted messages. The i^{th} experiment in the game proceeds as follows:

- **Setup** - The challenger generates the public and secret keys and PK is passed to the adversary.

  $PK \leftarrow (PK_1, PK_2, \cdots, PK_t)$

  $SK \leftarrow (SK_1, SK_2, \cdots, SK_t)$

- **Query Phase I** - The adversary adaptively requests for the tokens of the predicates $P_1, P_2, \cdots, P_{q'} \in \Phi$, and the challenger responds with the corresponding tokens

  $TK_j \leftarrow GenToken(SK, P_j)$.

- **Challenge** - The adversary chooses two data-biometric pairs (M_0, B_0) and (M_1, B_1) subject to the following restrictions:

  - $P_j(B_0) = P_j(B_1)$ for all $j = 1, \cdots, q'$.
  - If $M_0 \neq M_1$, then $P_j(B_0) = P_j(B_1) = 0$ for all $j = 1, \cdots, q'$.

  In i^{th} experiment, the challenger constructs the following ciphertexts:

  $$C_j \leftarrow \begin{cases} Encrypt(PK_j, M_0) & \text{if } P_j(B_0) = 1 \quad \text{and } j \geq i \\ Encrypt(PK_j, M_1) & \text{if } P_j(B_1) = 1 \quad \text{and } j < i \\ Encrypt(PK_j, \perp) & \text{o/w,} \end{cases}$$

and returns $C \leftarrow (C_1, C_2, \cdots, C_t)$.

- **Query Phase II** - The adversary can request more tokens for predicates $P_{q'+1}, \cdots, P_q \in \Phi$ as long as they adhere to the above restrictions.

- **Guess** - The challenger flips a coin $\beta \in \{0, 1\}$ and gives $C_* = Encrypt(PK_{B_\beta}, M_\beta)$ to the adversary, who returns a guess $\beta' \in \{0, 1\}$ of β. The advantage of adversary in attacking the system is defined as

  $Adv = |Pr(\beta = \beta') - \frac{1}{2}|$.

If Exp^i is the probability that the adversary guesses $\beta' = 1$ in experiment i, in a chain of $t + 1$ experiments, the adversary's advantage can be calculated by the differences in the outer experiments

$$Adv = |Exp^1 - Exp^{t+1}| \leq \sum_{i=1}^{t} |Exp^i - Exp^{i+1}|.$$

Since the public key system is semantically secure, $|Exp^i - Exp^{i+1}|$ and consequently adversary's advantage are negligible, which make the Φ-searchable system secure.

Bibliography

[1] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7905–7916, 2015.

[2] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant correlation analysis for feature level fusion with application to multimodal biometrics," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2016, pp. 1866–1870.

[3] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "Identification using encrypted biometrics," in *International Conference on Computer Analysis of Images and Patterns*. Springer, 2013, pp. 440–448.

[4] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1984–1996, 2013.