BUSITEMA UNIVERSITY
Pursuing Excellence

FACULTY OF ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING

FRAMEWORK FOR DETECTING AND EXTRACTING FILES HIDDEN BY ENCRYPTION AND STEGANOGRAPHY ON ANDROID DEVICES.

CASE STUDY UGANDA

BY

IKWAP FLAVIA AGATHA

BU/GS16/MCF/3

BIT (HONS) – MAK

A Dissertation Submitted to *the Directorate of Graduate Studies, Research and Innovation* in Partial Fulfillment of the Requirements for the Award of the Degree of Master of Computer Forensics of Busitema University

September 2019

DECLARATION

I declare that this dissertation has been composed solemnly by me and that it has not been submitted in whole or as part in any previous application for the award of a master's degree except where stated or otherwise by reference or acknowledgement. The work presented is entirely my own.

SIGNED

.....

Ikwap Flavia Agatha

Reg.No: BU/GS16/MCF/3

Faculty of Engineering

Department of Computer Engineering

Busitema University

APPROVAL

This Dissertation has been submitted for examination with the approval of my supervisors.

SUPERVISOR

Dr. Wilson Babu Musinguzi

Dean and Senior Lecturer, Faculty of Engineering

Signed ..... Date 11/09/2019

SUPERVISOR

Mr. Bwire Felix

Senior Lecturer, Faculty of Engineering

Department of Computer Engineering

Signed ..... Date 11/09/2019

DEDICATION

First of all, I dedicate this work to my beloved Husband Mr. Mudehere Francis for all the support he rendered to me through my studies. To my wonderful mother for all her support, encouragement and prayers. With great love I also dedicate this work to my lovely Children; Mukisa Patricia, Aviela Hannah Hwebasa, and Husinza Othniel who always missed me during the effort of this study, and special thanks to Gloria Athieno for all the support she extended to me.

ACKNOWLEDGEMENT

I thank The Almighty God who has given me strength to conduct this research.

In a very special way I thank my lecturers and supervisors; Dr. Wilson Babu Musinguzi, Mr. Bwire Felix and Mr.Ocen Gilbert for their collective efforts in guiding me throughout this dissertation, I have surely come this far because of your relentless support.

I am grateful to the teaching staff and Head of department Information Technology Uganda Christian University for their encouragements. To Mrs Gimuguni Lillian, who in the first place encouraged me to enroll for my Masters degree.

To my classmates Halongo Godfrey, Nafuye Ivan, Kisembo Moses, and to my friends Amutosi Evelyne, Nafuna Mercy, Ariokot Scholastic, Otim Lois, Mayi Beatrice and all others who have been there for me in different capacities, continue the good work.

I convey my utmost gratitude to my Husband; Mr. Mudehere Francis, to my mother Mrs Ikwap Hellen Rose, my brothers and sisters, to my lovely children and to my cousin Gloria Athieno. I am grateful to you all for your great support.

GOD BLESS YOU

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

Stego	Steganography
DLL	Dynamic Link Library
JPG	Joint Photographic Experts Group
MD	Message Digest Algorism
LSB	Least Significant Bit
RAM	Random Access Memory
UFED	Universal Forensic Extraction Device.
iOS	iphone Operating System
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
SSH	Secure shell
UDP	User Datagram Protocol

ABSTRACT

Anti-forensics aims at getting rid of all traces of digital evidences, nullify the data or increase the complexity of the investigation. In data hiding anti-forensics techniques of encryption and steganography, the evidence is completely out of view and therefore an investigator will not be able to use it in the investigation process. The evidence is not eliminated from the device, it's not even destroyed, however; it is just made less visible to the investigator. Algorithms that combine the two techniques of encryption and steganography have also become popular, making it even more difficult for digital investigations. This Research has developed an easy to use framework for detecting and extracting files (potential evidence) hidden by both anti-forensics techniques of symmetric encryption and steganography, an extension of Android Mobile Forensic Analyzer for Stego Data [7].

CHAPTER ONE

1.1 INTRODUCTION/BACKGROUND

A new wave of crime has become prevalent; Crime committed within digital domains. Criminals are using technology to facilitate their offenses and avoid being reprimanded creating new challenges for law enforcement agents [1]. Computer forensics is a discipline that uses "Computer forensic tools for collecting, analyzing, and presenting digital evidence to the courts of law" [2]. However, as computer forensic community develop and effectively put into use Forensics tools to carb computer crime, computer criminals are developing anti-forensics techniques to frustrate acquisition, retrieval, preservation and analysis of digital evidence [8].

Anti-forensics (AF) is a collection of tools and techniques that frustrate forensic tools, investigations and investigators [2]. Four primary goals for anti-forensics: Avoid being uncovered, disrupt the collection of evidence, increasing the time that an examiner needs to spend on a case, and cast doubt on a forensic report. [2]. Anti-forensics Techniques are majorly categorized into four types which include;- Destroying evidence, Hiding evidence, Eliminating evidence and Fabricating evidence [8].This research focuses on, Anti-forensics data hiding techniques of encryption and steganography on Android Devices.

There has been an explosive growth in Android system (especially for phones) usage for the past years which trend is expected to continue over the coming years [3] [4]. For instance Android phones with increasing storage capacity and functionality have out numbered the use of other computing devices and are becoming the primary choice for personal communication among the world's population, unfortunately, with the growth and popularity of Android phone usage, there has been a similar increase in the use of such devices for conducting digital crimes [3] [4].

Hiding information ensures that it is completely out of view and less likely to be incorporated into the forensic process. The information is not removed from the device, it's not destroyed or manipulated however; it is just made less visible to the investigator. To hide evidence, Files can be placed in unusual places to exploit limitations of the digital forensics software, or can be renamed to take advantage of the inherent blind spots of the investigator, techniques like Encryption and Steganography are commonly used to hide potential incriminating evidence [5]. When the two are combined they make a forensic investigation difficult if not impossible.

References

[1] John R. Vacc, *Computer Forensic : Computer Crime Scene Investigation Second Edition*. 2005.

[2] S. Garfinkel, "Anti-Forensics : Techniques , Detection and Countermeasures," *2nd Int. Conf. i-Warfare Secur.*, pp. 77–84, 2007.

[3] S. Azadegan, W. Yu, H. Liu, M. Sistani, and S. Acharya, "Novel anti-forensics approaches for smart phones," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 5424–5431, 2012.

[4] K. J. Karlsson and W. B. Glisson, "Android anti-forensics: Modifying cyanogenmod," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 4828–4837, 2014.

[5] E. Casey, *Digital Evidance And Computer Crime*. 2011.

[6] K. Rawat and S. Sah, "A Study- To Combined Cryptography and Steganography Methods," vol. 4, no. 5, pp. 2347–2350, 2016.

[7] W. T. Mambodza and A. R. Nagoormeeran, "Anti-forensic : Design and Implementation of an Android Forensic Analyzer," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 4, no. 4, pp. 2014–2020, 2015.

[8] G. Abboud, J. Marean, and R. V Yampolskiy, "Steganography and Visual Cryptography in Computer Forensics," pp. 25–32, 2010.

[9] J. E. Wingate, G. D. Watt, M. Kurtz, C. W. Davis, R. Lipscomb, and R. Lipscomb, "Defending Against Insider Use of Digital Steganography," no. c, 2007.

[10] M. Al-Hadadi and A. AlShidhani, "Smartphone Forensics Analysis: A Case Study," *Int. J. Comput. Electr. Eng.*, vol. 5, no. 6, pp. 576–580, 2013.

[11] The Computer and Missuse. Act, "Act 2 Computer Misuse Act," vol. CIV, no. 2, pp. 1–24, 2011.

[12] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," *Digit. Investig.*, vol. 3, no. SUPPL., pp. 44–49, 2006.

[13] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic

science through a new extended, granular taxonomy," *Digit. Investig.*, vol. 18, no. December 2015, pp. S66–S75, 2016.

[14] S. M. A. Asbeh and S. M. Hammoudeh, "AES Inspired Hex Symbols Steganography for Anti- Forensic Artifacts on Android Devices," vol. 7, no. 5, pp. 319–327, 2016.

[15] B. Chitradevi, N. Thinaharan, and M. Vasanthi, "Chapter 17 Data Hiding Using Least Significant Bit Steganography in Digital Images," *Stat. Approaches Multidiscip. Res.*, vol. I, pp. 144–150, 2017.

[16] W. Mazurczyk and S. Wendzel, "Information hiding: challenges for Forensic Experts," *Commun. ACM*, vol. 61, no. 1, pp. 86–94, 2018.

[17] O. Osunade and I. A., "Enhancing the Least Significant Bit (LSB) Algorithm for Steganography," *Int. J. Comput. Appl.*, vol. 149, no. 3, pp. 1–8, 2016.

[18] Kavitha, K. Kadam, A. Koshti, and P. Dunghav, "Steganography Using Least Signicant Bit Algorithm," *Int. J. Eng. Res. Appl.*, vol. 2, no. 3, pp. 338–341, 2012.

[19] "Least Significant Bit Steganography Technique for Hiding Compressed Encrypted Data Using," vol. 76, no. 10, pp. 12205–12231, 2017.

[20] M. Piccinelli and P. Gubian, "Detecting Hidden Encrypted Volume Files via Statistical Analysis," vol. 3, no. 1, pp. 30–37, 2013.

[21] S. Lowman, "The Effect of File and Disk Encryption on Computer Forensics," *http//lowmanio. co. uk/. Acesso em*, vol. 7, no. January, p. 7, 2010.

[22] W. Stallings, *C RYPTOGRAPHY AND.* .

[23] A. J. Raphael, "Cryptography and Steganography – A Survey by Raphael," vol. 2, no. 3, pp. 626–630.

[24] A. M. A. Brifcani and W. M. A. Brifcani, "Stego-Based-Crypto Technique for High Security Applications," *Int. J. Comput. Theory Eng.*, vol. 2, no. 6, pp. 835–841, 2013.

[25] K. Challita, H. Farhat, and N. Dame, "Combining Steganography and Cryptography : New Directions," *Int. J. New Comput. Archit. Their Appl.*, vol. 1, no. 1, pp. 199–208, 2011.

[26] M. A. A. Pujari and M. S. S. Shinde, "Data Security using Cryptography and Steganography," *IOSR J. Comput. Eng.*, vol. 18, no. 04, pp. 130–139, 2016.

[27] R. Chen and C. Yang, "Research on Android Anti-Forensic Tools Research on Android Anti-Forensic Tools," 2011.

[28] A. Distefano, G. Me, and F. Pace, "Android anti-forensics through a local paradigm," *Digit. Investig.*, vol. 7, no. SUPPL., 2010.

[29] B. Byrd, B. Zhou, and Q. Liu, "Android System Partition to Traffic Data ?," vol. 3, no. 2, 2017.

[30] F. Length and O. Hashvalue, "Cryptography hash functions," pp. 1–16.

[31] A. Kak, "Lecture 15 : Hashing for Message Authentication Lecture Notes on ' Computer and Network Security ' by Avi Kak (kak@purdue.edu) Goals : • The birthday paradox and the birthday attack • Crypto Currencies and Their Use of Hash Functions • Hash functions fo," pp. 1–95, 2018.

[32] O. Dunkelman, "Hash Functions — MD5 and SHA1," pp. 1–15, 2012.

[33] Access Data, "MD5 Collisions," *Computer (Long. Beach. Calif).*, no. April, 2006.

[34] N. Tech and M. Kishore, "Signing Message Using Fast MD5 Hashing Digital Signature Algorithm," vol. 1, no. 7, pp. 5–8, 2012.

[35] E. Benkhelifa, B. E. Thomas, L. Tawalbeh, and Y. Jararweh, "A framework and a process for digital forensic analysis on smart phones with multiple data logs," *Int. J. Embed. Syst.*, vol. 10, no. 4, p. 323, 2018.

[36] M. Yates and H. Chi, "A framework for designing benchmarks of investigating digital forensics tools for mobile devices," p. 179, 2011.

[37] C. R. Prabhu and P. Savaridassan, "AN ANTI-FORENSICS APPROACH FOR ANDROID OS," vol. 2, no. 2, pp. 45–51, 2014.

[38] I. Sporea, B. Aziz, and Z. Mcintyre, "On the Availability of Anti-Forensic Tools for Smartphones," *Int. J. Secur.*, vol. 6, no. 4, pp. 58–64, 2012.

[39] I. U. Akarawita, A. B. Perera, and A. Atukorale, "ANDROPHSY - Forensic framework for Android," *15th Int. Conf. Adv. ICT Emerg. Reg. ICTer 2015 - Conf. Proc.*, no. August, pp. 250–258, 2016.

[40] M. Prof and S. M. A. Burney, "INDUCTIVE & DEDUCTIVE RESEARCH APPROACH 06032008.pdf," no. March, 2008.

[41] V. L. Plano Clark and J. W. Creswell, *Understanding Research: A Consumer's Guide, (2nd Edition)*, vol. 30, no. 6. 2015.

[42] A. R. Hevner and S. T. March, "Design Science in Information Systems Research Design Science in Information Systems Research," no. 520.

[43] S. Y. R. Esearch, B. A. R. Hevner, S. T. March, J. Park, and S. Ram, "D ESIGN S CIENCE IN I NFORMATION," vol. 28, no. 1, pp. 75–105, 2004.

[44] C. Fisher, *Researching and Writing a Dissertation - for business students*. 2007.

[46] R. V. KREJCIE and D. W. MORGAN, "Determining sample size for research activities. Educational and psychological measurement," *Rna*, vol. 30, no. 3, pp. 607–610, 1970.

[47] K. S. Taber, "The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education," *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1273–1296, 2018.

[48] D. G. Bonett and T. A. Wright, "Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning," *J. Organ. Behav.*, vol. 36, no. 1, pp. 3–15, 2015.

[49] C. S. 637 - 642. Wells and J. A. Wollack, "An Instructor's Guide to Understanding Test Reliability," *Test. Eval. Serv.*, pp. 2–5, 2003.

[50] R. Heale and A. Twycross, "Validity and reliability in quantitative studies," *Evid. Based Nurs.*, vol. 18, no. 3, pp. 66–67, 2015.

[51] C. Liu, S. Li, S. Qin, and S. Yang, "Research and Application of Influences of Lateral Pressure Coefficients on the Extension Angle of Coal Cracks," *Math. Probl. Eng.*, vol. 2016, no. 3, pp. 1–10, 2016.

[52] XRY Mobile Forensic Tool, https://www.msab.com, accessed 10/03/2019