The International Journal of Multi-Disciplinary Research

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

DEVELOPING A DESKTOP CRYPTOSTEGANOGRAPHIC SECURITY APPLICATION

(Conference ID: CFP/702/2018)

By: Lameck Mwilu

Student: Information Security and Computer Forensics

School of Engineering,

Information and Communication University,

Lusaka, Zambia

ABSTRACT

Information is a very important asset. In businesses, information is often one of the most important assets a company possesses because it differentiates companies and provides leverage that helps one company become more successful than another. Because of this scenario, Information is always vulnerable to attack. This paper discus some techniques that safeguards information from attack through a developed Cyptosteganographic Desktop Security Application. Efforts have been made to foster file security through the development of different desktop security applications and these applications employs different security modules in their implantation. This paper gives an in-depth study and examines a selected number these desktop security application in reviewing their performance and recognizing their shortfalls the perpetuated to the development of Cyptosteganographic Desktop Security Application.

As it may be noted, most system compromise occurs via Network and Desktop Security breach. This always gives attackers authorized access to sensitive information. Hence, this paper examines how files containing sensitive information can be secured to detour unauthorized access through a comprehensive step by step procedure. It further gives an overview of the development process and the four security implementations at each given layer in the Cryptosteganographic Desktop Security Application. Finally, this paper addresses the significance, challenges and opportunities circled around the developed Security Application.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

DEDICATION

This dissertation is dedicated to my father, Mr. Lameck Mwilu (smr). He has been instrumental and instilled the value that education is the best equalizer.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

ACKNOWLEGEMENT

This work is the result of extensive research and I would never have survived the research period, let alone produced this work, had it not been for the wonderful support and friendship of many people. Likewise, my success at University of Zambia has been supported by many people and in no particular order; I would like to thank the following:

My supervisor, Mrs. David Zulu, for the insightful comments and valuable supervision throughout, steering me in the right direction, enriching my mind, and broadening my horizons.

My friends Jessie Musonda and Jason Chirwa, for the love, care and support that kept me going through the best of times and the darkest of hours.

My Mentor Evangelist Benson Chisenga for the much needed fatherly love and insightful guidance in all aspects of my life. His unfailing desire to see everyone do well is worth a great commendation.

My family and particularly my brothers and sisters. I am forever grateful to them.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

TABLE OF CONTENTS

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

WORKING DEFINITIONS

Cryptography is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text).

Steganography is hiding data within data. It is the practice of concealing a file, message, image, or video within another file, message, image, or video.

Encipher is converting (a message or piece of text) into a coded form.

Decipher is converting a text written in code, or a coded signal into normal language.

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

Hacker is a computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem.

Intruder is a person who goes into a place where they are not supposed to be

Vulnerability is a weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorized actions within a computer system.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

INTRODUCTION

Information can be classified into different categories. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse, hence the need to enforce security to such information.

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Steganography and Cryptography. Basically, the purpose of cryptography and steganography is to lender a given file a secret. However, steganography is not the same as cryptography. Cryptography hides the contents of a secrete message from a malicious people, whereas steganography even conceals the existence of the message. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used.

It is possible to combine the techniques by encrypting a file using cryptography and then hiding the encrypted file using steganography. Henceforth, the realization of this combination is sets the baseline for this project.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

PROBLEM STATEMENT

Unauthorized access to sensitive information comes into play because of low level security implementation. Intruders find it easy to penetrate the security layer on a protected file or information. This scenario is evident because most desktop security application are belt on low level security, most application consist of two to a single layer of security. In order to combat this serge, we have developed a high-level security application that can be implemented. With Steganography in particular, many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

So, we prepare this application, to make the information hiding simpler and user friendly.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

AIMS/RATIONALE

The main aim of this project is to;

- Develop a high-level desktop security application capable of protecting resident and information under transmission from being read and understood and being accessed by anyone except the authorised user.

This is made possible by implementing a four-layered security model which will compliment encryption and decryption through possible examination of existing desktop security applications that employ cryptography and steganography techniques.

OBJECTIVES

The main objectives of this project include:

- To examine popular desktop applications the employ Cryptography and Steganography techniques in accessing their vulnerabilities.
- To explore and implement techniques of hiding data using encryption module
- To explore extraction techniques of getting secret data using decryption module.
- To combine cryptography and steganography techniques in the development a desktop security application.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

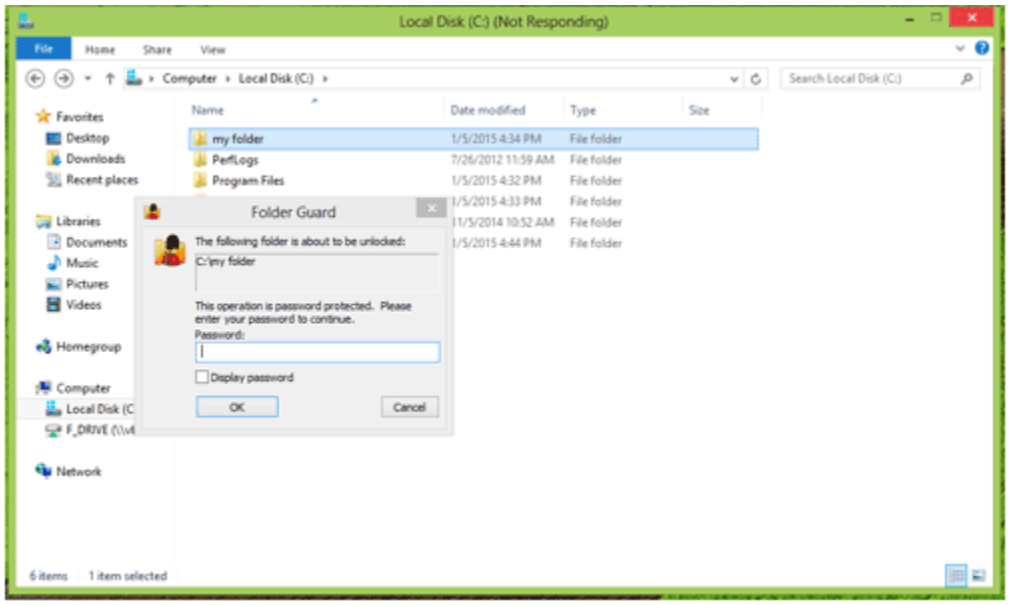
REVIEW OF LITERATURE

In this project research, two most used and renowned application software are reviewed to access their efficiency, effectiveness and technologies used in relation to the developed application. These include:

FOLDER GUARD

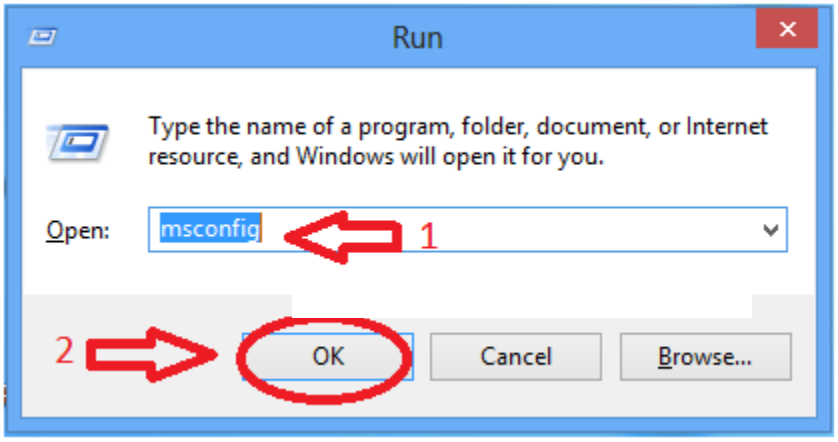
Folder Guard is a computer security application developed by Winability Software. It controls access of files and Folders through hiding and encryption, rendering the invisible until a correct password is entered. Folder Guard locks files and folders with passwords, to stop other users from peeking the records. One can completely hide private folders from virtually all applications, and such folders would remain invisible until a valid password is entered. Despite its strong security techniques, folder guard has a major security problem because one can open a folder secured by Folder guard with no problem as demonstrated below;

OPENING A FOLDER GUARD PASSWORD PROTECTED FOLDER WITHOUT A PASSWORD.

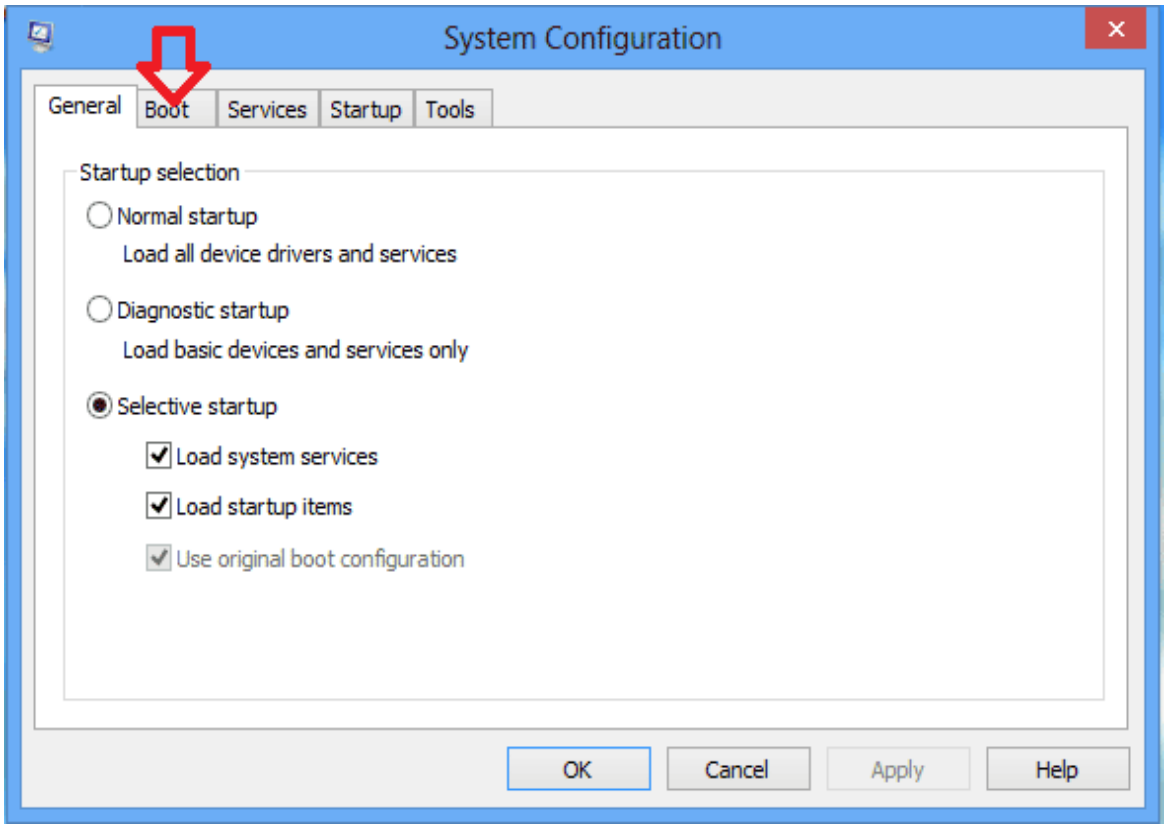


1. Press **Windows + R** key together
2. Windows **RUN** dialog box will appear type "msconfig" in the box without the quotes and click **OK** to continue.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

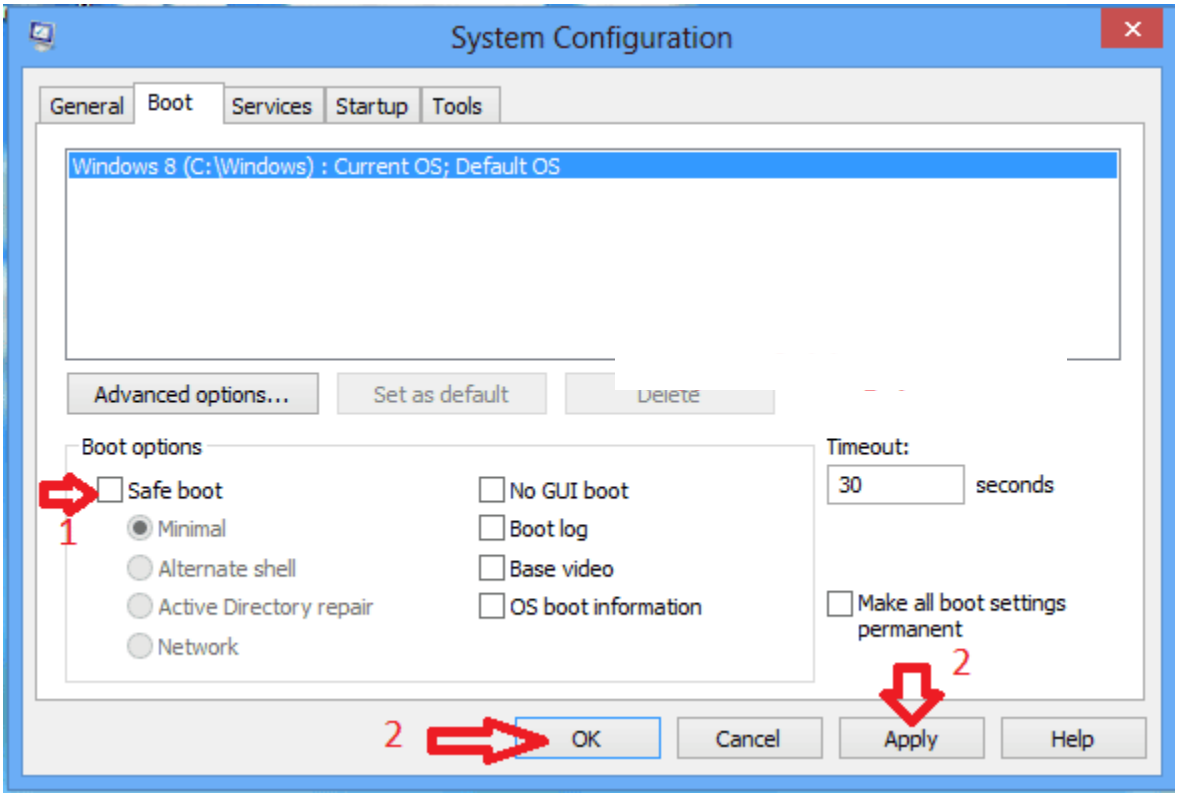


3. System Configuration Box will appear, click on **Boot** tab

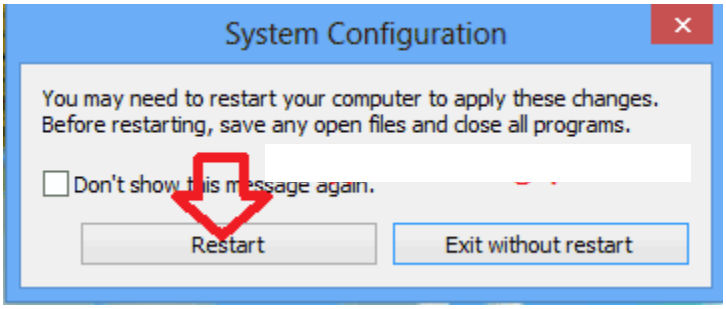


4. Choose boot option "safe mode" then click on **APPLY** and **OK**

ISSN: 3471-7102, ISBN: 978-9982-70-318-5



5. Click Restart



6. Windows will start in **Safe Mode**
7. Now you can open Folder Guard protected folder without a password.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

From this examination, it is evident that Folder Guard doesn't offer the best solution to desktop security.

WISE FOLDER HIDER

Wise Folder Hider is a security app that has been designed to password-protect folders and files, so that prying eyes are unable to read or modify them. The app provides security for files and folders on Windows PC, blocking any unauthorized access and securing privacy. Wise folder hider can also protect removable drives. Despite its robust security implementation, the also has a loophole using the procedure below;

1. Click **Start** > Open Run dialog > Type: **regedit** and hit Enter;
2. Open **Registry Editor** and go to: HKEY_CURRENT_USER;
3. Click **Software** > **new software** > **Wise Folder Hider** > **Uninstall**;
4. Edit the value to **0**;
5. Go to **Control Panel** and **uninstall Wise Folder Hider**;

Through this procedure you render the password parameter of the protected folder to zero, hence you can open without a password.

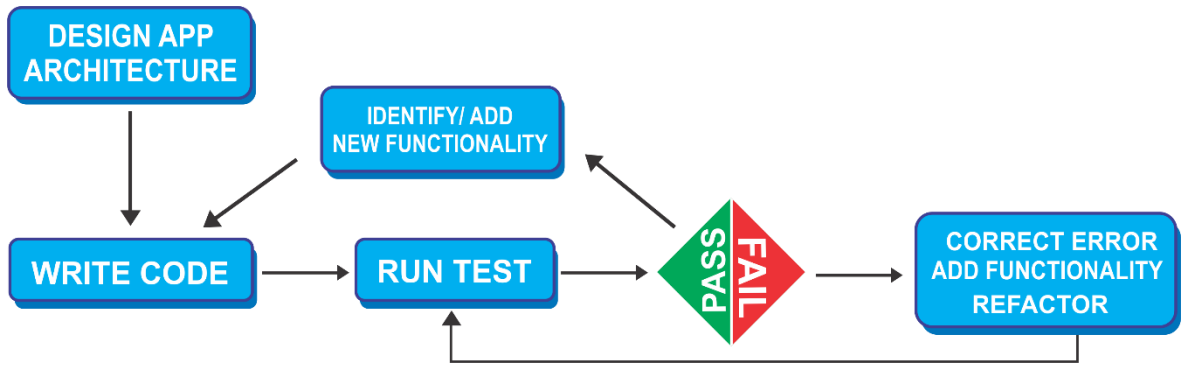
These two Security applications are the most robust and popular, the only limitation is their security porousness and they don't employ steganography in their security implementation. From this in-depth discovery, we have strived to develop a desktop application with countermeasures the limitations.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

METHODOLOGY

APPLICATION DEVELOPMENT METHODOLOGY

Test-driven development (TDD) is an approach that was adopted for the development of this application. The code was developed incrementally, along with a test for the increment. Moving to the next increment was made possible only after the code developed passes the test. The diagram below describes this development methodology;



TEST DRIVEN DEVELOPMENT (TTD) METHODOLOGY Designed by Lameck Mwilu @ICU Zambia

PROGRAMMING LANGUAGE

The proposed Programming Language to be used in the development of this security application is C♯ because:

- It has a huge standard library with so much useful toolsets well-implemented and easy to use.

APPLICATION DEVELOPMENT ENVIRONMENT

MICROSOFT VISUAL STUDIO ENTERPRISE 2015

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Microsoft visual Studio is It has a rich and powerful development integrated development environment (IDE) from Microsoft. It is used to develop Computer programs for Microsoft windows, as well as web sites, web apps, web services and mobile apps.

CORE SECURITY IMPLEMENTATION

ROBUST FORENSICS: A FOUR LAYERED DESKTOP SECURITY APPLICATION

Robust Forensics is the name given to the desktop application because of its robustness and efficiency. This application will has incorporated the four layers of security as described below. This is in a view of meeting the defined standard of a high-level security application.

LAYER 1. CRYPTOGRAPHY

This layer of implementation will incorporate:

Encipher: to make the message unreadable to all but the intended user

Decipher: to undo the encipherment and make the message readable

LAYER 2. ENCRYPTION

This layer of implementation will incorporate:

Encrypt: implementation of a secret code to transform data into a secret coded

Decrypt: to transform encrypted data back to its unencrypted form using a secret key

LAYER 3. IMAGE STEGANOGRAPHY

This layer of implementation will incorporate:

Hide file in image: hiding a confidential text file into an image

Unhide file from image: retrieval of a hidden a file from an image

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

LAYER 4. FILE STEGANOGRAPHY

This layer of implementation will incorporate:

Hide the file: rendering the confidential file invisible

Unhide the file: retrieving the invisible file invisible

SYSTEM DESIGN AND ANALYSIS

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt.

Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. I used this tool in this software called "Steganography" that is written in C#.Net language and you can use this software to hide your information in any type of pictures without any converting its format to BMP (software converts inside it).

The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So, every step we go to upper layer image quality decreases and image retouching transpires.

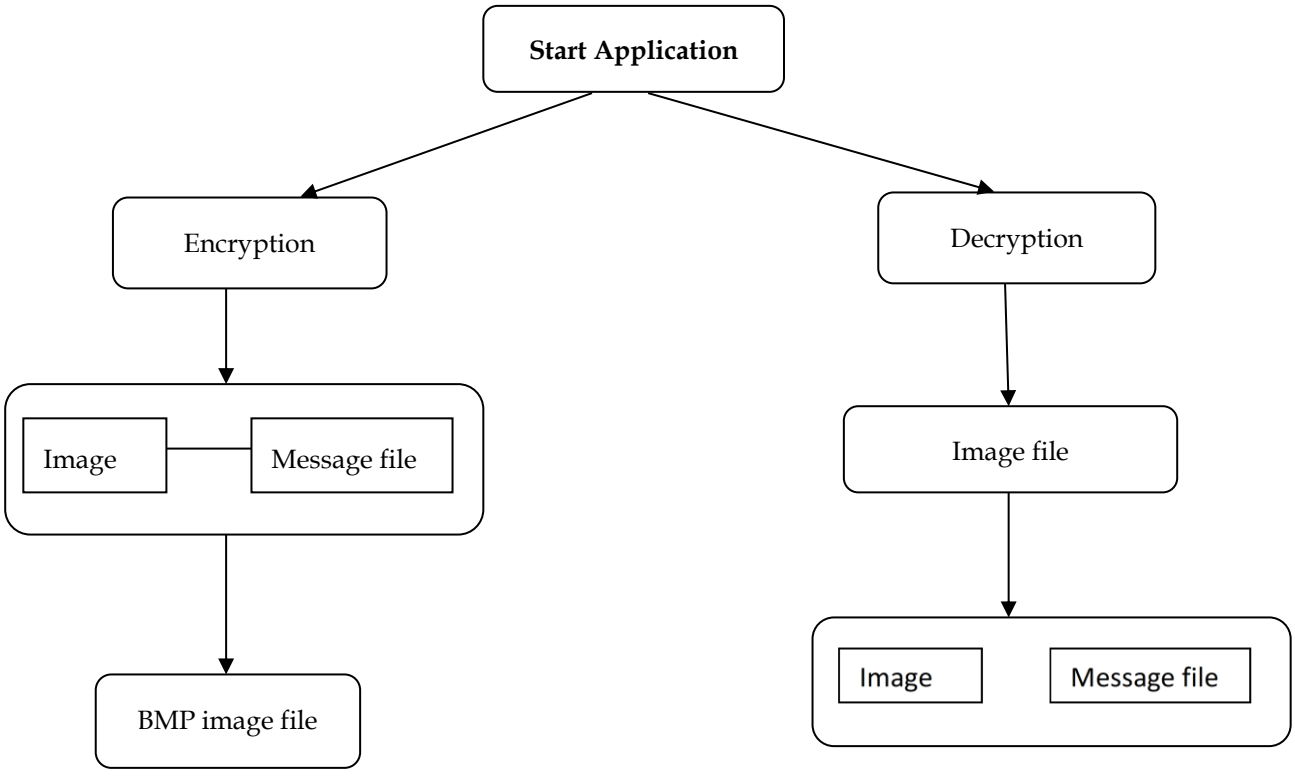
The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

The decrypt module is used to get the hidden information in an image file. It takes the image file as an output, and give two files at destination folder, one is the same image file and another is the message file that is hidden it that.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Before encrypting file inside image we must save name and size of file in a definite place of image. We could save file name before file information in LSB layer and save file size and file name size in most right-down pixels of image. Writing this information is needed to retrieve file from encrypted image in decryption state.

The graphical representation of this system is as follows:

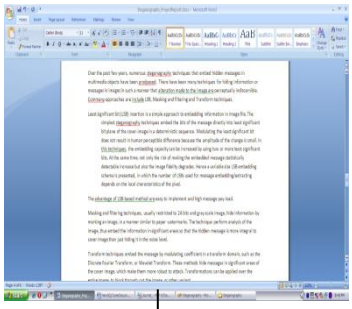


ISSN: 3471-7102, ISBN: 978-9982-70-318-5

ENCRYPTION PROCESS

IMAGE FILE

INFORMATION FILE

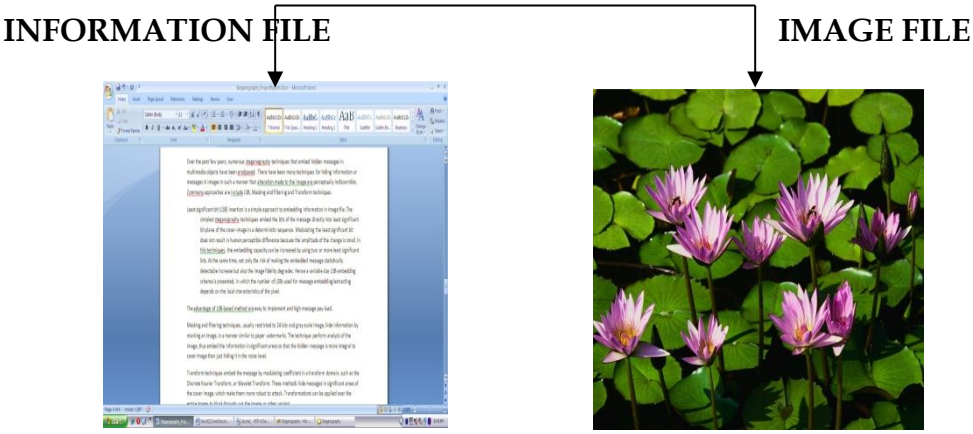


BMP FILE

DECRYPTION PROCESS

BMP FILE

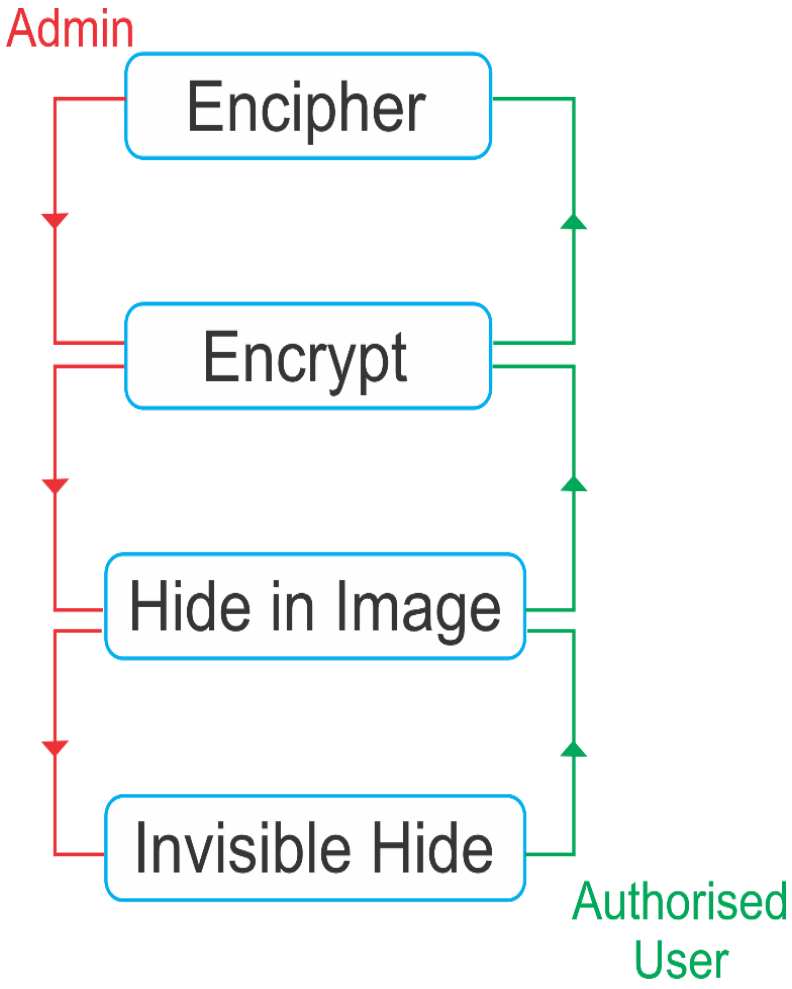
ISSN: 3471-7102, ISBN: 978-9982-70-318-5



USE CASE MODEL

This Use Case Model describes the four-security operation that the user who is denoted as the administrator can implement in order to secure the intended file containing sensitive information. The admin privileges are denoted in red whilst the authorized user is denoted in green. For an authorized user to gain access to the file containing sensitive information he has to undergo the four-security layered using the access keys provided by the Admin.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5



ISSN: 3471-7102, ISBN: 978-9982-70-318-5

PROGRAMMING ALGORITHM

This Programming algorithm describes the exact steps needed for the computer to perform a given functionality or reach a goal. This step by step procedure described the entire application functionality.

Step 1: Start

Step 2: Encipher file content information and move to Step 4, otherwise move to Step 10

Step 3: Decipher File content Information and move to step 10

Step 4: Encrypt file by forming a password and or move to Step 6, otherwise move to step 10

Step 5: Decrypt file by entering a correct password and move to step 10

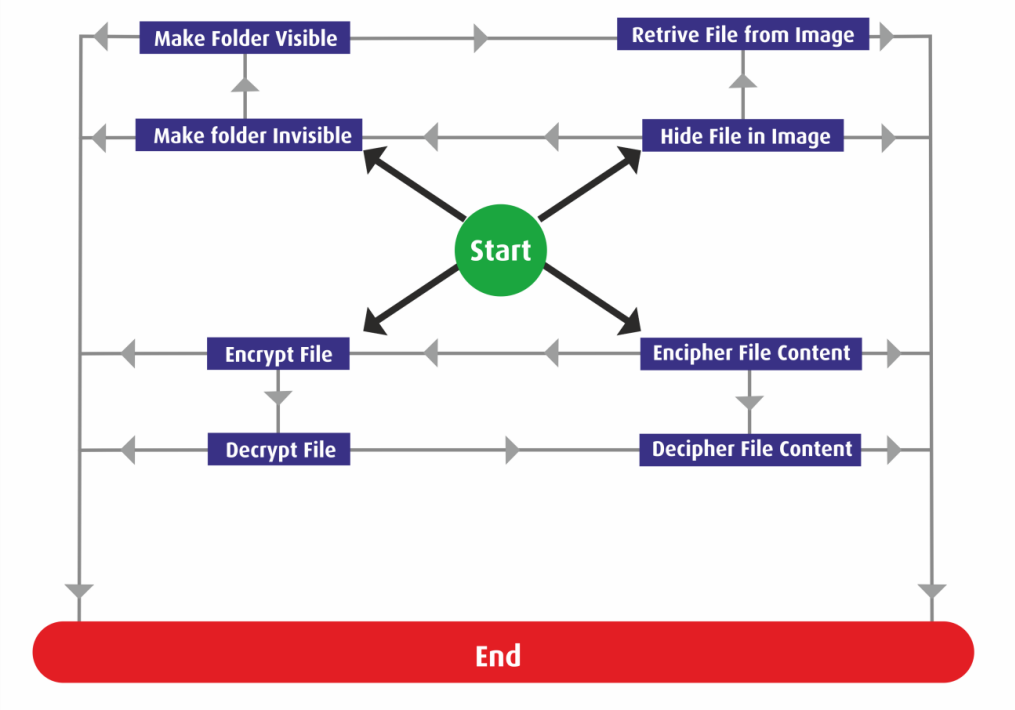
Step 6: Hide enciphered file in an image and move to step 8, otherwise move to step 10

Step 7: Retrieve the hidden file form image and move to step 10,

Step 8: Hide the Image containing the file in a folder rendered in visible and move to step 10

Step 9: Make visible the folder containing the image file and move to step 10

Step 10: End



ISSN: 3471-7102, ISBN: 978-9982-70-318-5

GRAPHICAL USER IINTERFACE (GUI) DESIGN

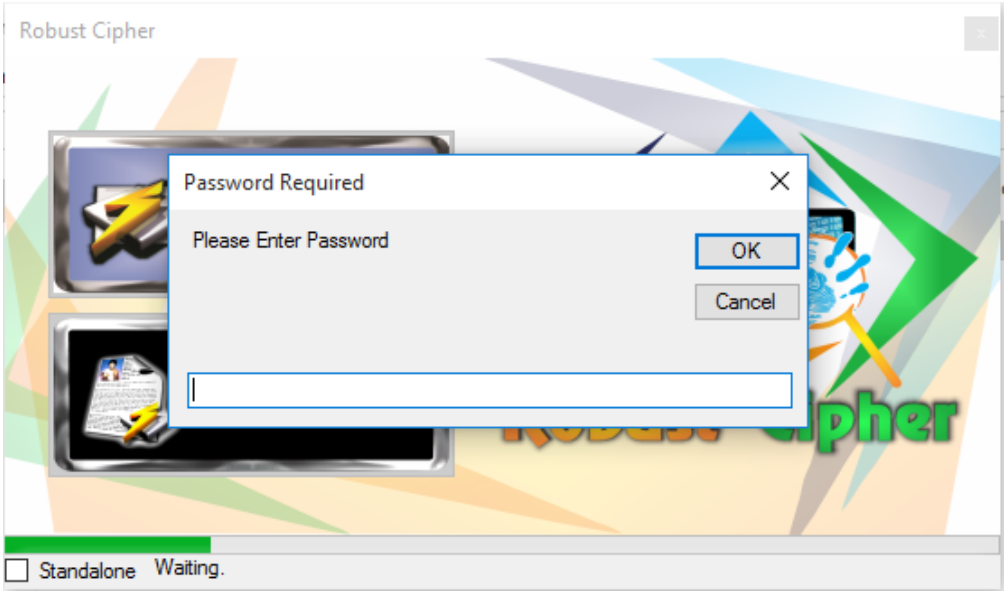
This is the first screen which has four-tab options – Encipher and Decipher, Encrypt and Decrypt, Hide in Image and Hide in Folder. It also has the online button where is redirects you to an online platform of Robust Forensics.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

ENCIPHER AND DECIPHER

When you click on the Encipher and Decipher tab, a new window opens.

When you click on the Cipher tab, it takes you to a directory where the folder that contains the file whose information needs to be ciphered is located. Once you select the folder, a set password dialog box appears



A user password is set and the information becomes enciphered

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

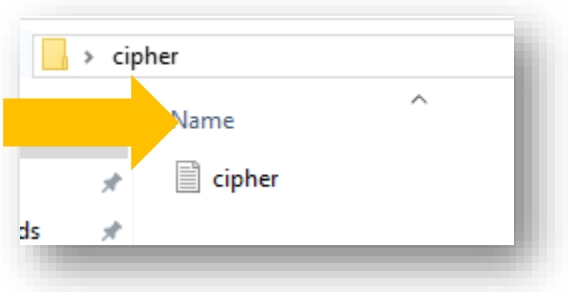
To make the information readable again, an authorized user has to go the decipher process and enter a correct password.

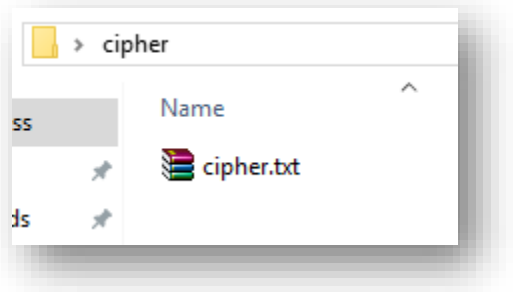
ENCRYPTION AND DECRYPTION

From the first window, when you click on the Encrypt and Decrypt tab, a new window opens

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

When you click on the Encrypt tab, it takes you to a directory where the folder that contains the file whose information needs to be Encrypt is located. Once you select the folder, a set password dialog box appears. When a password is set the file become a compressed file which requires a password to unzip it.





To have access to the encrypted file, an authorized user has to go through the decryption process and enter a correct password.

HIDE IN IMAGE

From the first window, when you click on the Hide in Image tab, a new window opens

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

To load an Image, click "Browse" that is next to the Load Image textbox. Go to a directory where the Image you intend to use is located and select the Image file which you want to use hide information and click on Open button.

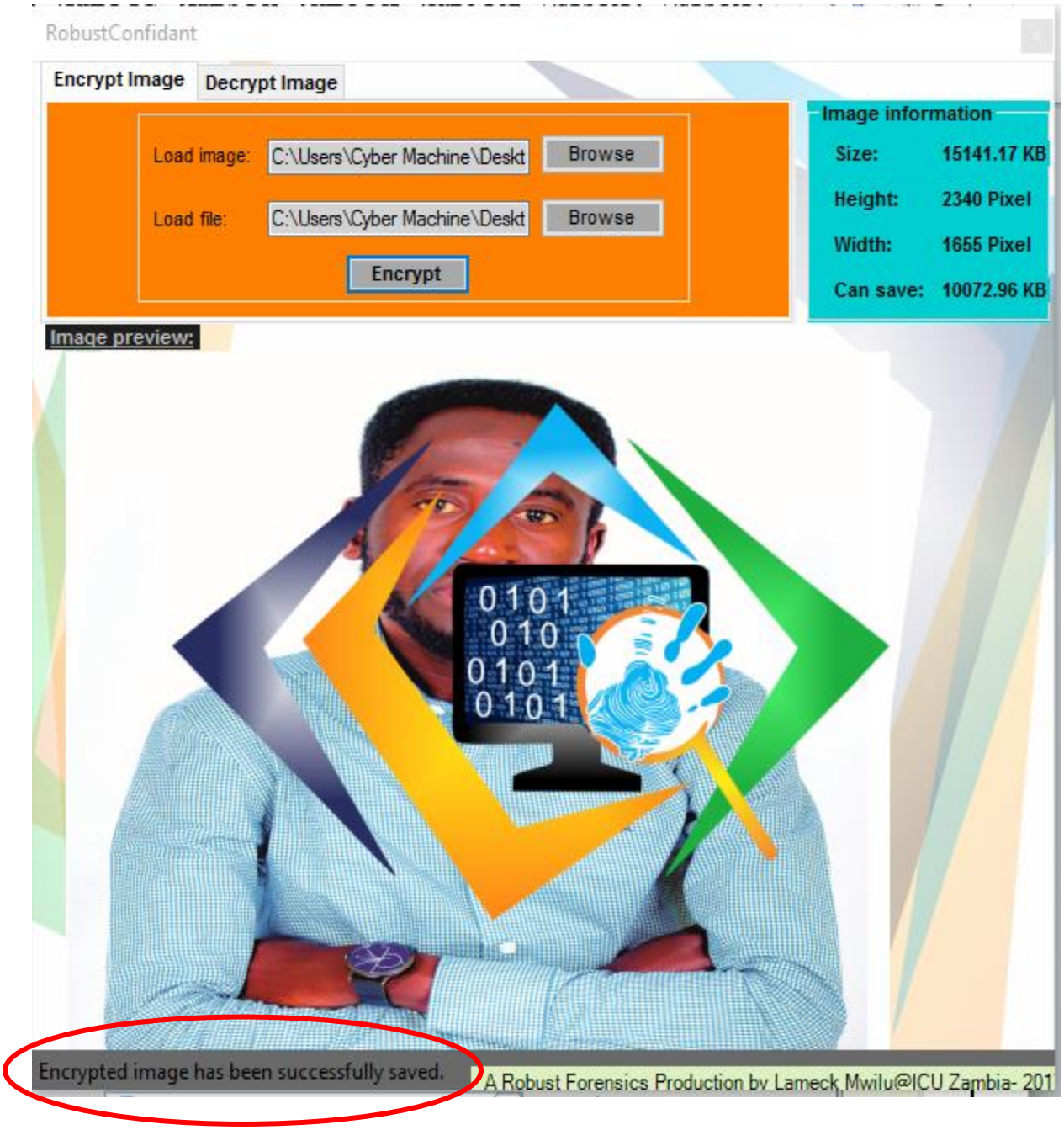
The image file will open and is displays as follows. Next, click on "Browse" button that is next to the Load File textbox.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Go to a directory where the file you intend to hide in image is located and and click on Open button.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

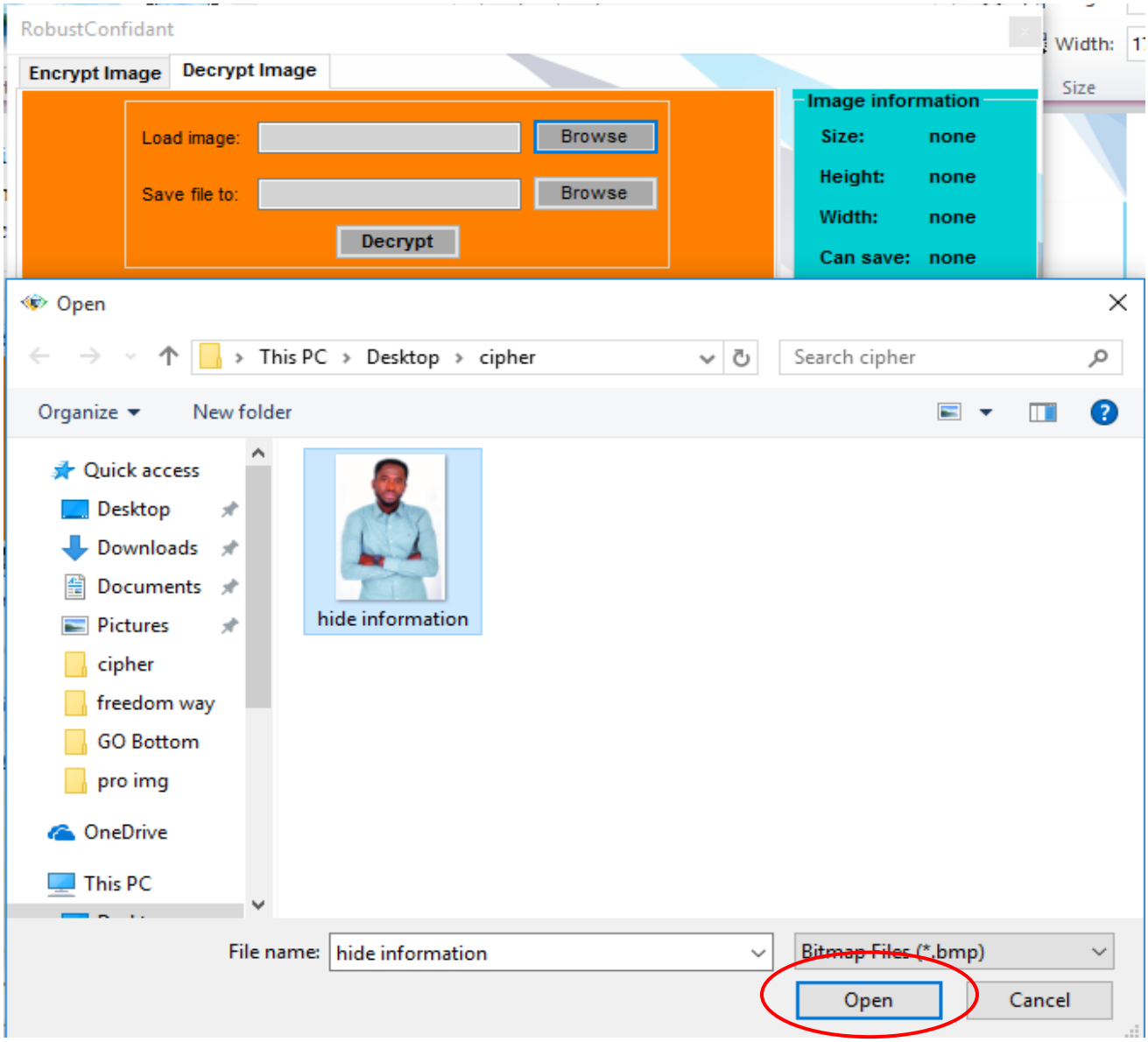
When the two files are loaded, click the Encrypt button and you will be directed to choose a location where you intend to save the new image with hidden information in it. A new copy of the image will be created with a default image format of BMP.



ISSN: 3471-7102, ISBN: 978-9982-70-318-5

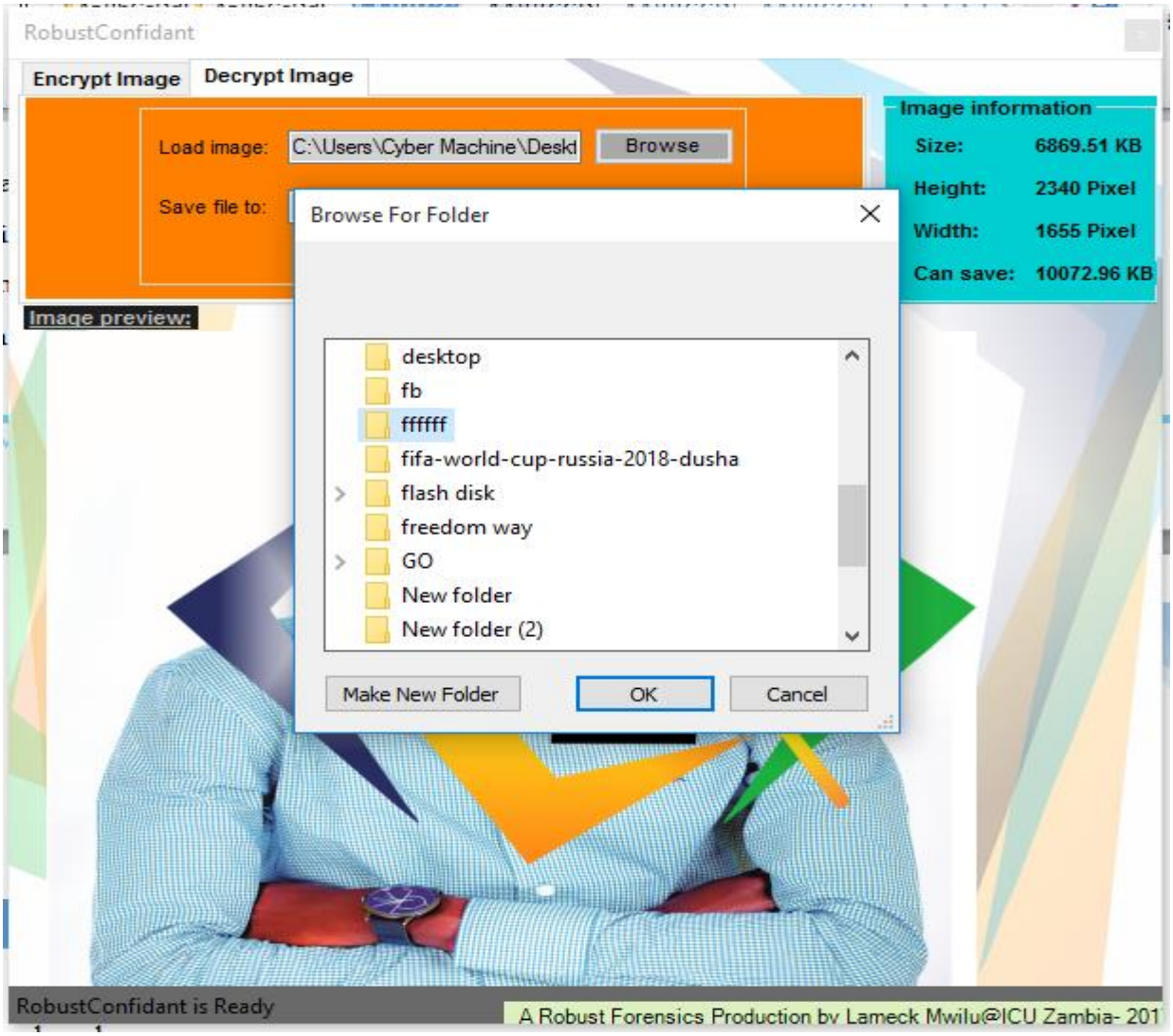
To retrieve the file from the image, click on “Decrypt Image” tab

Next click on the “Browse” button, which open the Open file dialog box, here you have to select the image which is Encrypted and has hidden information file. Select the image file and click on Open button.



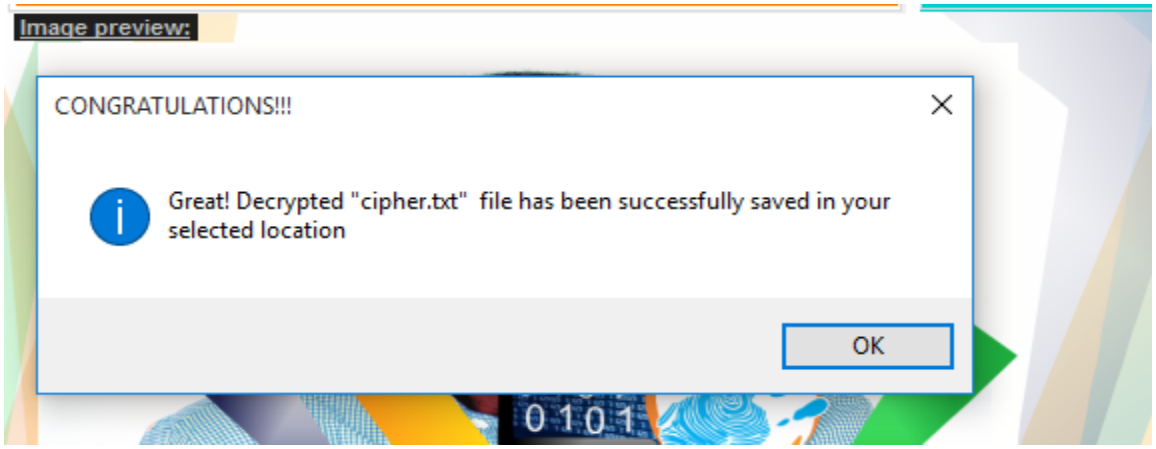
ISSN: 3471-7102, ISBN: 978-9982-70-318-5

The image will be load in the application. Now click on "Browse" button which is next to "Save file to" textbox. It will open a dialog box that is "Browse for folder". It ask you to select the path or folder, where you want to extract the hidden file. Select the folder and click on Ok button.



ISSN: 3471-7102, ISBN: 978-9982-70-318-5

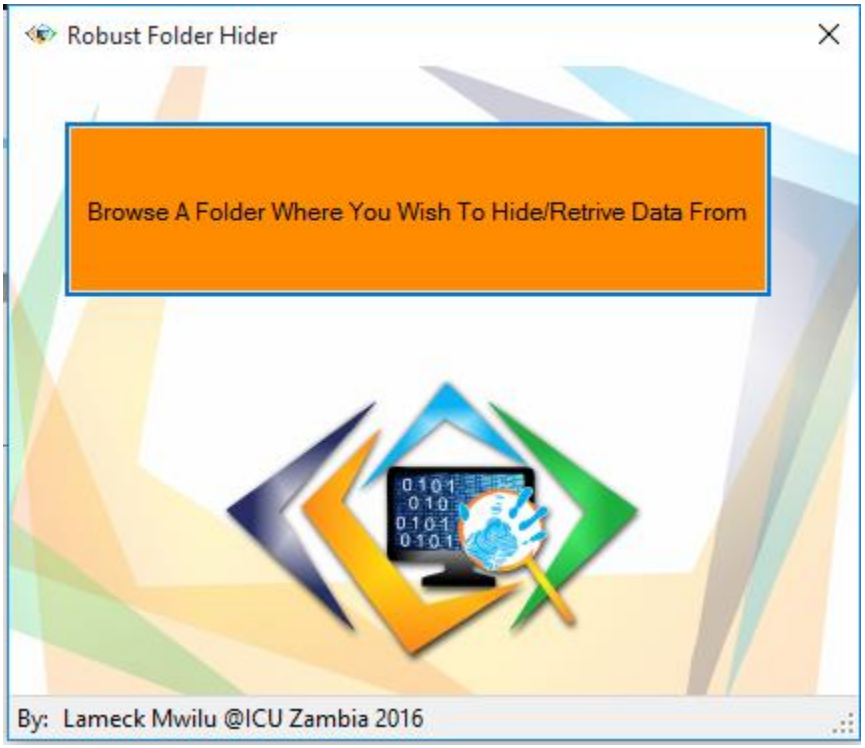
Click on Decrypt button, it will decrypt the image, the hidden file and image file is saved into selected folder. A message will pop out to congratulate you on your success.



Click **OK** to Close.

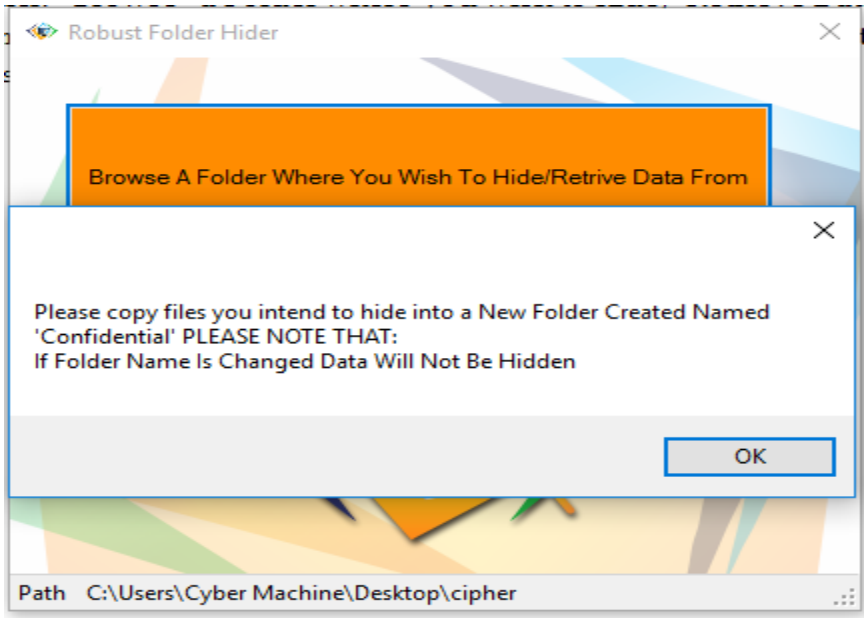
HIDE IN FOLDER

From the first window, when you click on the Hide in Folder tab, a new window opens



ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Click "Browse "a Folder where you wish to hide/ Retrieve Data From". Go to a directory where the folder you intend to hide is located and click on Open button. A message with instructions will pop up.



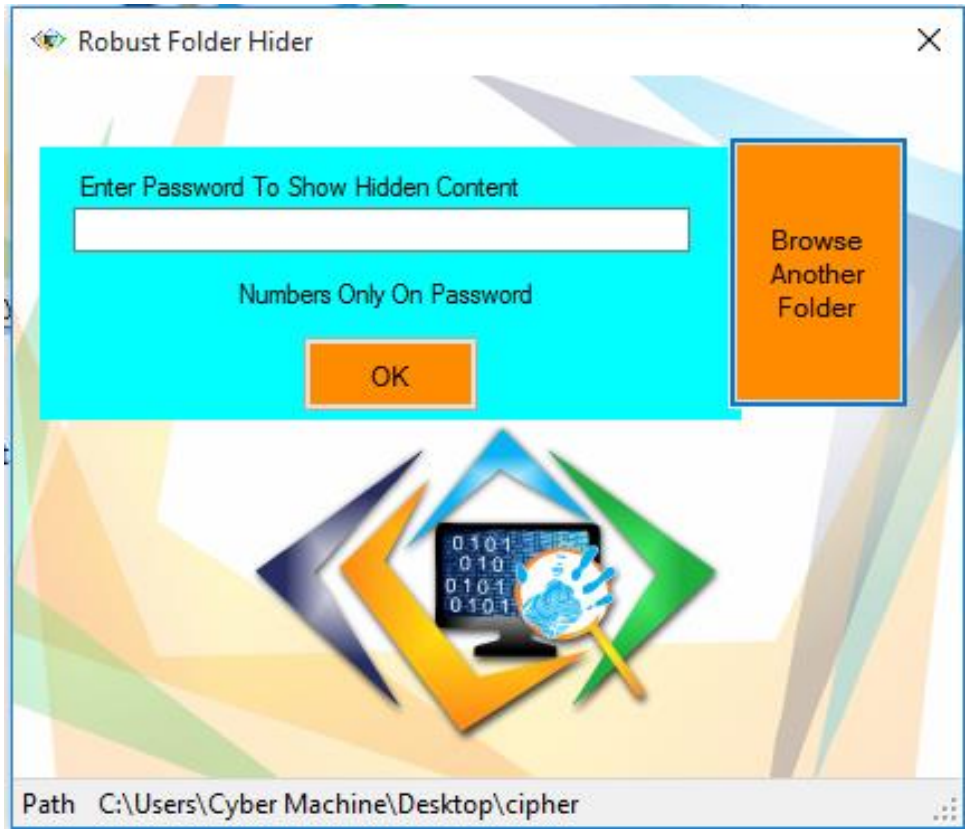
Copy the contents you wish to hide into a folder created named **Confidential** and enter password.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

The Folder named Confidential will disappear

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

To retrieve the confidential folder from its hidden state, start the application and browser to the directory where the confidential folder was located. Automatically, the application will detect that there is a hidden folder and an enter password dialog box will appear.



Enter a correct password and the confidential folder will appear. **DONE!**

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

SIGNIFICANCE/IMPLICATIONS

The developed Desktop Security Application will play an important role in securing sensitive information. Henceforth, deterring hackers from achieving their mischievous ambition

It is also right to not that despite the significance of this security application, once it lands in wrong hands it can be used to the disadvantage to the authorized user. Such a scenario can result into a denial of service attack because illegitimate users will not have the privileges to access their information. The authorized users can also lose access to their information in an event that they forget the password to opening the secured files. So it is highly advisable that the configured passwords be kept with strict security measure with almost remembrance.

Its four layered security implementations will tighten the security of sensitive information. For an unauthorized user to access the restricted information, he must be well equipped in undergoing the security measure under each layer of security. The other essence of increasing the layers of security is to make an unauthorized user give up in an event that they decide to crack down the enforced security. This means that they have to undergo through the four layers of security which might be viewed as an unachievable task because chances of giving up along the way are high.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

CONCLUSION

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography and cryptography is not just limited to military or espionage applications. Steganography and cryptography play an increasing role in the future of secure communication in the "digital world".

Since information is an important asset for distinct individuals and organizations, the call for proper security cannot be over emphasized. Therefore, the use of the developed desktop security application will prevent attacks especially insider threats. This will play a significant role in achieving the core requirement of the CIA triad which include; confidentiality, integrity and availability.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

REFERENCES

[1] A. B Ruighaver, S. B. M. S. C., 2007. Oganisational Security Culture: Extending the user- edn perspective. *Computers and Security,* Volume 26, pp. 56-62.

[2] A.B. Ruighaver, S. B. M. S. C., 2007. Organisational Security Culture: Extending the end user perspective. *Computers and Security,* Volume 26, pp. 56-62.

[3] Anon., 20`3. *Free Download Manager.* [Online]
Available at: http://en.freedownloadmanager.org/Windows-PC/Folder-Guard.html
[Accessed 14 April 2017].

[4] Anon., 2016. *File Hippo.* [Online]
Available at: http://filehippo.com/download_wise_folder_hider/
[Accessed 14 April 2017].

[5] Casey, E., 2011. *Digital Evidence and Computer Crime.* 3rd ed. s.l.:Academic Press.

[6] CRIME, U. N. O. O. D. A., 2013. *Comprehensive Study on Cybercrime,* Viena: United Nations.

[7] Easttom, C., 2012. *Computer Security Fundamentals.* 2nd ed. Indiana: Pearson Education, Inc..

[8] EC-Council, 2010. *Ehtical Hacking & Countermeasures- Secure Network Infrastructures.* New York: Course Technology.

[9] Edward, B. a., 2006. Organisational Security. *Key Dimensions of Organisational Security,* Issue 2, pp. 1-7.

[10] Jamie Graves CEO at ZoneFox, 2014. *Insider Threats: The Accidental Data Breach,* Atlanta Georgia: Linkedin.

[11] King, T., 2018. *EaseUS.* [Online]
Available at: https://www.easeus.com/file-recovery/recover-files-from-folder-lock-without-password.html
[Accessed 2018 08 12].

[12] Kizza, J. M., 2014. *Computer Network Security and Cyber Ethics.* 4th ed. Noth Carolina: McFarland & Company, Inc.

[13] Kumar, P., 2018. *pcmobitech.* [Online]
Available at: https://www.pcmobitech.com/folder-guard-secret-open-folder-without-password/
[Accessed 12 08 2018].

[14] Ousley, M. R., 2013. *Information Security - The Complete Reference.* 2nd ed. Nwe York: The Grew Hill Education.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

[15] Peltier, T. R., 2014. *Information Security FUNDAMENTALS.* 2nd ed. New York: CRC PressTaylor & Francis Group.

[16] Prowse, D. L., 2012. *CompTIA Security+ SY0-301 Authorized Cert Guide.* 2nd ed. Indiana: Pearson Education, Inc..

[17] Richard O'Hanley, J. S. T., 2014. *Information Security Management Handbook.* 6nd ed. New York: CRC PressTaylor & Francis Group.

[18] Ronald L. Krutz, R. D. V., 2003. *The CISSP Prep Guide: Gold Edition.* 1st ed. Indiana: Wiley Publishing.

[19] Sandywell, 2010. the Internet and new criminality. In: &. Jewkes , ed. *On the globalisation of crime.* Cullompton: Willan Publishing, pp. 97-102.

[20] Shuangbao (Paul) Wang, R. S. L., 2013. *Computer Architecture and Security- Fundamenttals of Designing Secure Computer Systems.* Singapore: John Wiley & Sons.

[21] Sommerville, I., 2011. *SOFTWARE ENGINEERING.* 9th ed. Boston: Addison Wesley.

[22] Stamp, M., 2006. *INFORMATION SECURITY PRINCIPLES AND PRACTICE.* 1st ed. New Jersey: JohnWiley & Sons, Inc.

[23] Thomas R. Peltier, J. P. J. B., 2005. *Information Security FUNDAMENTALS.* 1st ed. New York: AUERBACH PUBLICATIONS.

[24] Vincent Nestler, G. W. w. A. C., 2011. *Principals of Computer Security.* 2nd ed. s.l.:The Mc Grew Hill Companies.

[25] Vincent Nestler, W. A. C. G. W. M. H., 2011. *Principles of Computer Security: CompTIA Security+™ and Beyond Lab Manual.* 2nd ed. Chicago: The McGraw-Hill Companies.

[26] Walker, M., n.d. *Certified Ethical Hacker.* 2nd ed. s.l.:Mc Graw Hill Education.

[27] Whitten , J. L. & Bentley, L. D., 2008. *INTRODUCTION TO SYSTEMS ANALYSIS AND DESIGN.* New York: McGraw-Hill/Irwin.

[28] William Stallings, L. B., 2012. *COMPUTER SECURITY PRINCIPLES AND PRACTICE.* 2nd ed. indiana: Pearson Education, Inc.

[29] Wong, L., 2009. Computer Systems & Networks. 2 October, pp. 1-2.