Indian Journal of Fundamental and Applied Life Sciences ISSN: 2231– 6345 (Online)
An Open Access, Online International Journal Available at www.cibtech.org/sp.ed/jls/2014/04/jls.htm
2014 Vol. 4 (S4), pp. 646-651/Nik

Research Article

CRYPTOGRAPHY, ENCRYPTION/DECRYPTION AND STEGANOGRAPHY

***Keyvan Derakhshan Nik**
Kristianstad University, Sweden
**Author for Correspondence*

ABSTRACT

Nowadays, one of the fascinating sciences is information security around the world which covers vast variety of knowledge. It includes special knowledge about data protection. Cryptography and Encryption have been used for several centuries to protect data from hackers. From past few years, in lots of efforts scientists have been allocated to encrypted information in different ways 1. One of the methods which can be used in different approaches is Steganography. In the following, this paper will give some brief Introduction of Cryptography, Encryption/Decryption and Steganography with their usage Then It will continue with some statistics for knowledge of people and their idea about this concept as a case study. This paper will end up with a summary to obtain the importance of the Steganography for future science.

Keywords: *Cryptography, Encryption/Decryption, Steganography, Sound File, Image File, Text File*

INTRODUCTION

Introduction and Terminology

What is Cryptography?

“Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication”. In other words, Cryptography is a knowledge that is not relay on computer science. People usually use Cryptography in daily life. For example, when people tell some slangs or idioms, they try to hide a story or a concept inside that slang or idiom; therefore, they use Cryptography in their daily conversation. Another usage of Cryptography is in the war, where soldiers usually use Cryptography to communicate with others because they do not want to give information to their enemies.

What are Encryption and Decryption?

To Introduce the Encryption, we require knowing some other concepts here.

Scientists explain: “The original information to be hidden is called "plaintext"”[3].

On the other hand, ”The hidden information is called "ciphertext"”[3].

Now we can explain Encryption as any procedure or task to convert Plain text into Cipher text. In addition, scientists define another concept like Decryption which is explained as any task or process to convert cipher text into plain text.

Encryption and Decryption usually are used in computer science to make secure connection between client and server. There are some technologies for encrypting and decrypting data but one of the most famous groups among these technologies is “Hashing technology”[4].

What is Steganography?

“Steganography is the art or practice of concealing a message, image, or file within another message, image or file. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. ”[5]. In the modern technology everybody can hide information within image (.bmp , .gif,…) file , audio file and other text file without attract hacker attention to this information. On the other hand, this method is so dangerous for terrorism attack, too. But we can use it in positive ways.

Scenario 1: People can have special digital image, sound or text for logging instead of using password for their email address. Therefore, sniffers cannot realize which part of data allocated to password. Moreover, this idea can expand to have both username and password in one file.

Scenario 2: Bank clients can have special image for connecting to their account as an excessive security layer. The Bank client can use this file for Internet connection authentication and authorization also they can use this file when they go to bank for any reason.

Scenario 3: People usually use ID card or Passport for illustration of their information to some organizations. This information could be hidden under one photo that every person can hold it in one file.

Statistics and Analyze Information (Case Study)

As a survey that I have done among my friends who have profile in the Internet, I have obtained very interesting results. The survey is done within 30 people who are between 20 and 60 years old. Figure 1 shows the percentage of people who are in different age in this survey.

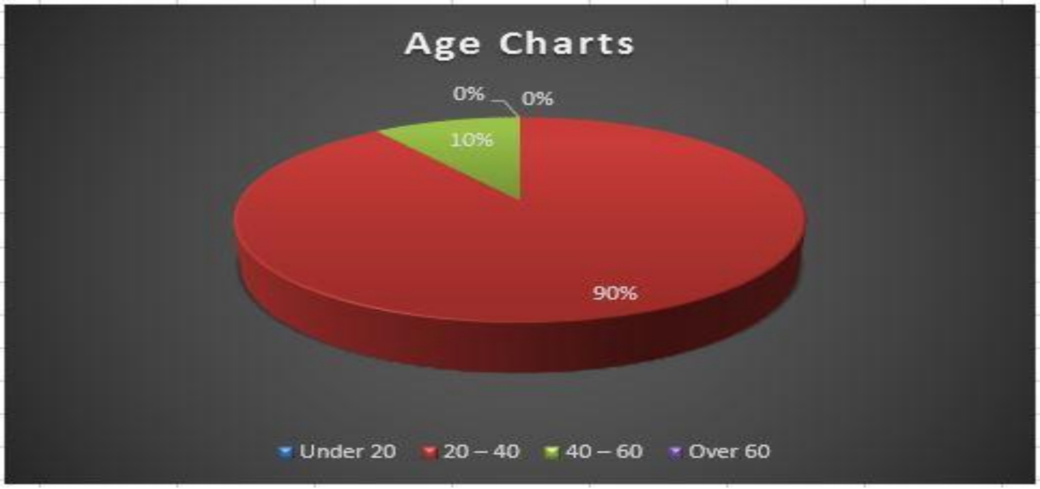

Figure 1: Age groups percentage

As we can see in figure 1, 90% of people who cooperate in this survey are between 20 and 40 years old. At the first step, we asked some questions to know the knowledge of our population about Cryptography, Encryption/Decryption and Steganography, and how many have computer skills.

In figure 2, we can obtain the percentage of people who have computer skills and others.

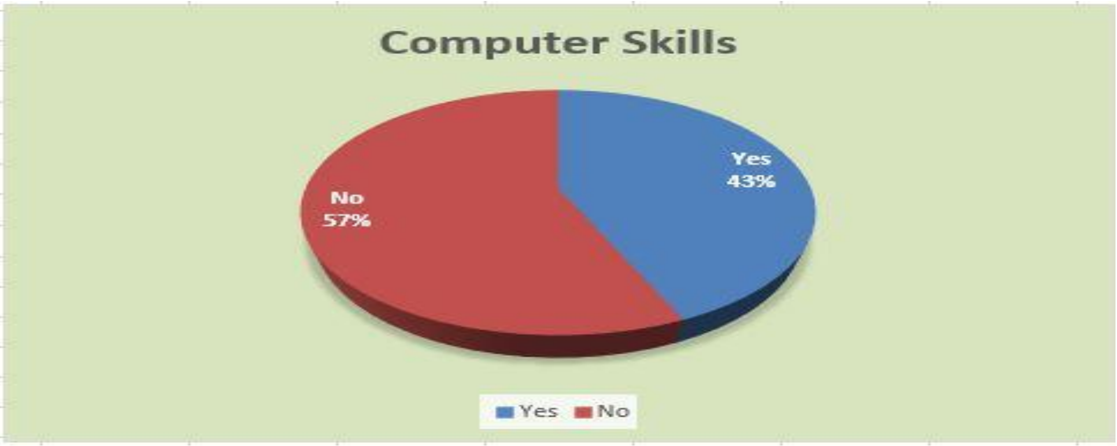

Figure 2: Computer Skills of volunteers

In this survey, we asked volunteers to answer some questions about Cryptography, Encryption/Decryption, Steganography definitions. There are some results about knowledge of these concepts which are illustrated in figure 3, 4, 5.

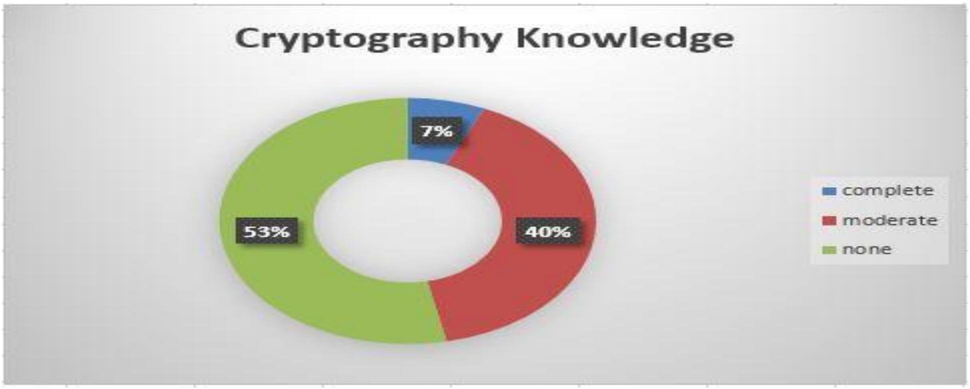

Figure 3: Percentage of Cryptography Knowledge

Figure 3 shows more than half of people do not know anything about Cryptography while it is not allocated to computer science while only 7 percent of people know Cryptography completely.

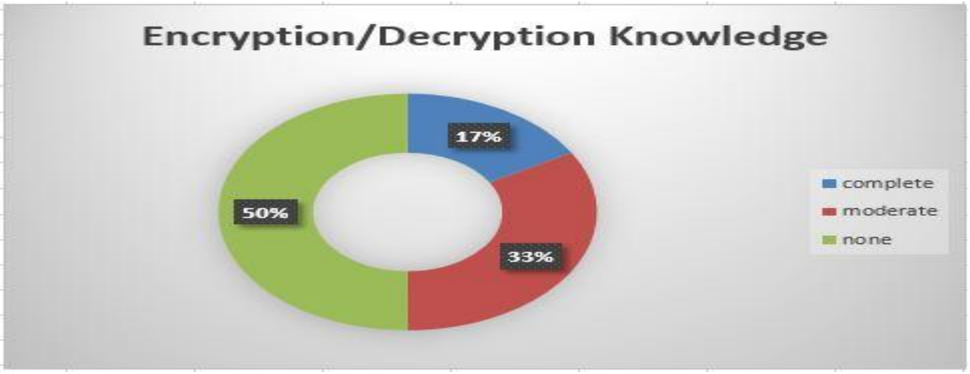

Figure 4: Percentage of Encryption/Decryption Knowledge

Figure 4 depicts one half of people know Encryption /Decryption concepts while it is one of the most important computer science concept. On the other hand, we saw in our population there are around 40 % of people have computer skills (Figure 2). It can prove this idea that Encryption/Decryption is one of attractive concept for non-computer skills people.

On the other hand, this concept is more popular for people rather than Cryptography concept. Because 17% of people know Encryption/Decryption very well, but just 7% know Cryptography completely.

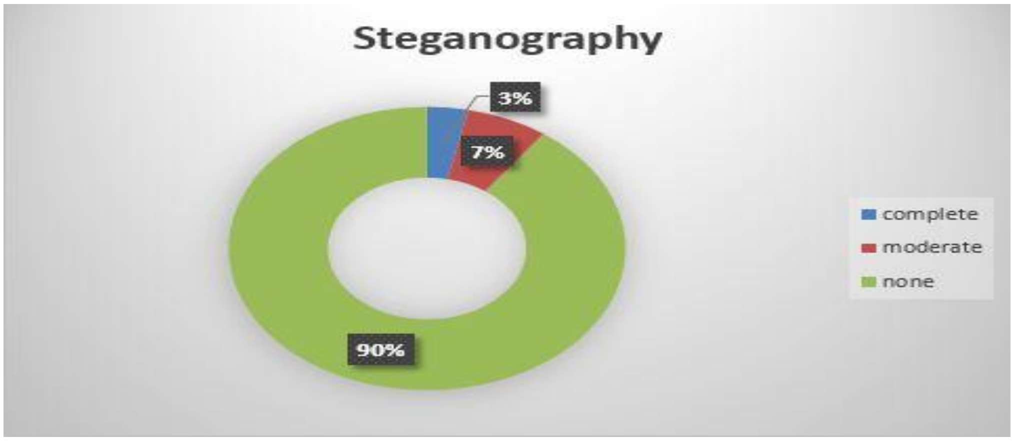

Figure 5: Percentage of Steganography Knowledge

Figure 5 demonstrates Steganography is not a well-known concept in our population because it is a really new concept compared to other concepts. Almost no one knows anything about that and just 7% of them have heard something about it and just 3% know it very well.

On the next step, we asked volunteers about their idea about possessing special file instead of password or username and password. Figure 6 illustrates the results.

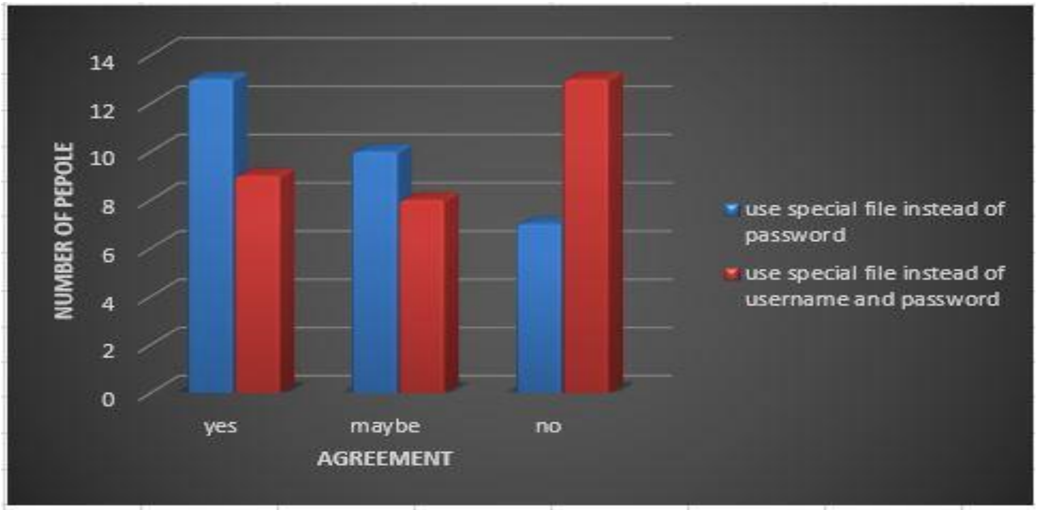

Figure 6: Agreement to have Special file instead of password or username and password

As above picture shows most people (13 out of 30 persons) would like to have special file instead of password which is the same quantity of people who would not like to have special file instead of username and password.

On the final step, we asked voluntaries to choose file types that they would like to use instead of their password or username and password. We put Image file, Sound file, text file and none of them (for persons who do not like to use these types of file or they are against this idea). The following pictures show the result.

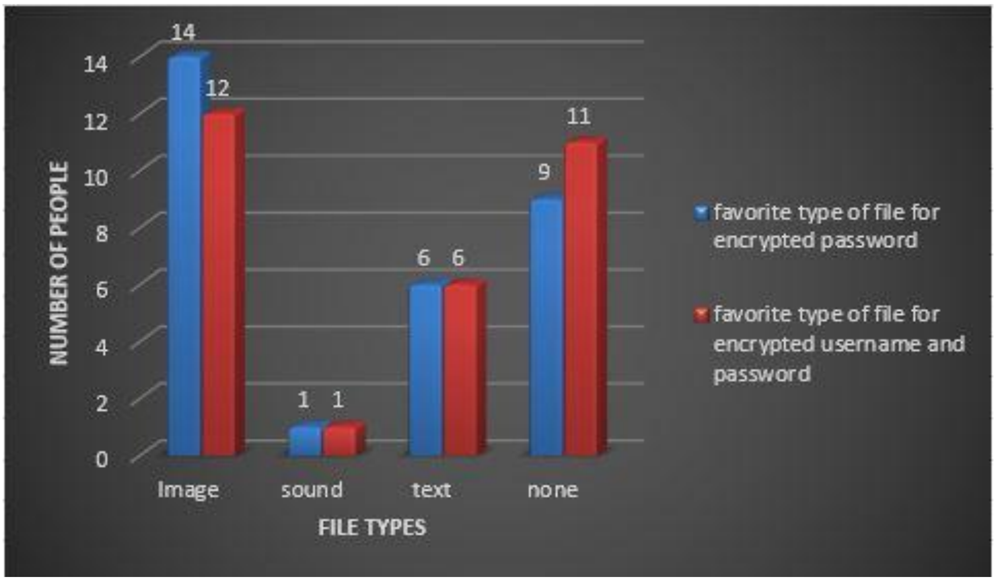

Figure 7: File types voluntaries select for password or username and password

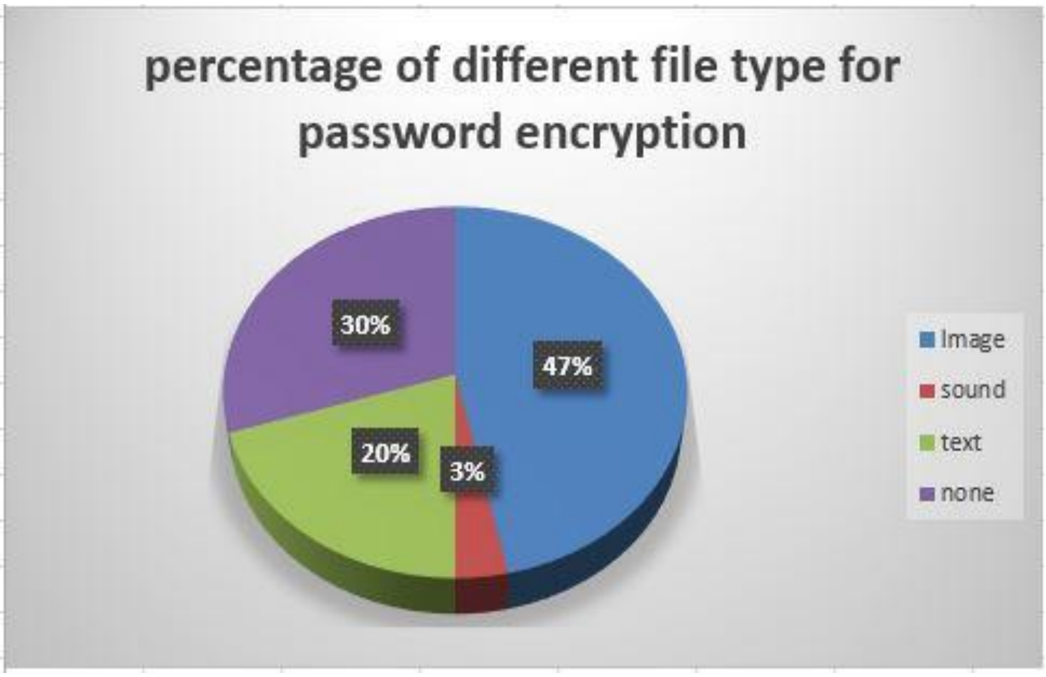

Figure 8: Percentage of different file types for just password encryption

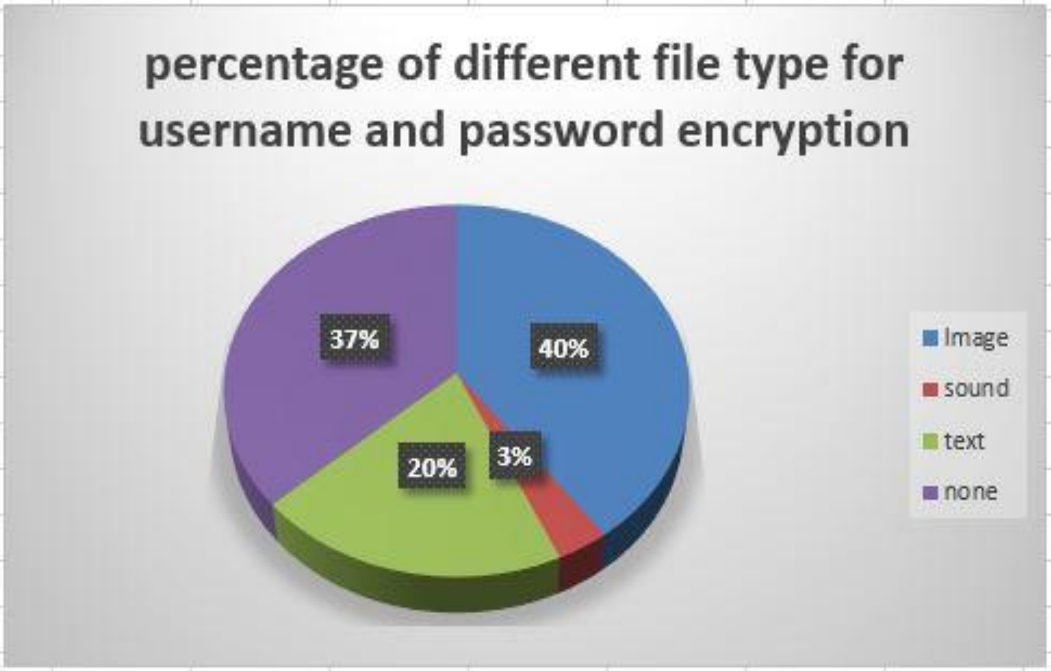

Figure 9: Percentage of different file types for username and password encryption

As we can see in Figures 7 and 8 most people would like to use image file instead of password by 14 out of 30 (47%) and sound file has the minimum proportion between all categories by 1 out of 30 (3%).

Also Figures 7 and 9 illustrate again almost maximum number of people would like to use image file instead of username and password by 12 out of 30 (40%). The second level allocated to people who would like to choose none of the file types for username and password encryption by 11 out of 30 (37%). Additionally, sound files stay at the same level as password encryption by 1 out of 30 (3%).

Summary

In conclusion, Cryptography was one of the oldest technologies which were used for encryption and it had been created by human before creating Encryption/Decryption concept. Afterwards, Encryption/Decryption was generated after computer invention. To follow this revolution, Steganography science is created to use for future.

There are lots of people who are not aware of the ability of Steganography and we can shake information security by using Steganography in our current affairs.

REFERENCES

Adam S (2006). Practical Aspects of Modern Steganography.

Amitava N, Saswati G, Sushanta B, Debasree S and Partha PS (2012). An Image Steganography Technique using X-Box Mapping, *IEEE-International Conference on Advances In Engineering, Science And Management*.

Ayushi (2010). A Symmetric Key Cryptographic Algorithm, *International Journal of Computer Applications* **1**(15) 0975 – 8887.

Koblitz N (1994). *A Course in Number Theory and Cryptography* (Springer-Verlag) New York, Inc.

Menzes AJ, Paul C, Van Dorschot V and Vanstone SA (2001). *Handbook of Applied Cryptography* (CRS Press) 5th Printing.

Nicholas GM (2005). Past, present, and future methods of cryptography and data encryption.

Peter Meyer (No Date). An Introduction to the Use of Encryption. Available: http://www.hermetic.ch/crypto/intro.htm.

PUB F (2012). National Institute of Standards and Technology Patrick Gallagher, *Federal Information Processing Standards Publication* 180-4 March.

Shannon CE (1949). Communication Theory of Security System, *Bell System Technical Journal* **28**(4) 656 – 715.

Stallings W (2002). *Cryptography & Network Security: Principals and Practice*, 3rd Edition (Prentice Hall).