Article Citation Format
Okyere, R.L. (2022): Efficient Data Hiding Scheme Using Steganography and
Cryptography Technique. Journal of Digital Innovations & Contemporary Research
in Science, Engineering & Technology.
Vol. 10, No. 2. Pp 25-32
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P4

Efficient Data Hiding Scheme Using Steganography and Cryptography Technique

Okyere, Rufus Larbi
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: rufus.okyere@stgimpa.edu.gh
Phone: +233244378932

ABSTRACT

Transportation of information across the internet necessitates security concerns. Internally, transmission of data in organisation must also be secured, according to security standards. In a typical distribution, all traffic transferred via the public network (Internet) is secured. However, sensitive information must not be easily accessible in the event that an attacker compromises any services on the hosts and gains access to their resources. The advancement of information technology has enabled large amounts of digital data to be reliably transported through unrestrained communication channels. Today's information world is a digital world. Data transmission over an unsecure channel is becoming a major issue of concern nowadays. And at the same time intruders are spreading over the internet and being very active. So to protect the secret data from theft, some security measures need to be taken. In order to keep the data secret various techniques have been implemented to encrypt and decrypt the secret data. Findings of this study show how steganography and cryptography techniques are used for efficient data hiding to prevent unauthorised access to confidential and sensitive information. The study present recommendation for policy and practice.

Keywords: Efficiency, Data Hiding Scheme, Steganography, Cryptography, Security

1. INTRODUCTION

The aim of this study is to understand efficient data hiding scheme that use steganography and cryptography technique. The advancement of information technology has enabled large amounts of digital data to be reliably transported through unrestrained communication channels (Horng et al., 2020). Today's information world is a digital world. Data transmission over an unsecure channel is becoming a major issue of concern nowadays. And at the same time intruders are spreading over the internet and being very active. So to protect the secret data from theft some security measures need to be taken. In order to keep the data secret various techniques have been implemented to encrypt and decrypt the secret data.

Information is becoming more valuable, and the creation, sharing, and utilization of information is becoming a more significant economic activity. Intellectual property law may provide protection for information, which is frequently traded as a good or service. Consumers need access to a wide range of information sources while information producers seek access to distribution channels. In addition, democracy's foundational component is the free flow of information (OECO, 2022). Information is becoming more valuable, and the creation, sharing, and utilization of information is becoming a more significant economic activity. Intellectual property law may provide protection for information, which is frequently traded as a good or service.

Consumers need access to a wide range of information sources while information producers seek access to distribution channels. In addition, democracy's foundational component is the free flow of information. As the value and volume of data transmitted and stored on information and communications networks rises, so does its significance for society and the global economy. Additionally, those systems and data are becoming more open to dangers including unauthorized access, usage, misappropriation, change, and destruction. While improving the utility of these systems, factors such as the proliferation of computers, rising computing power, interconnectedness, decentralization, expanding networks, and rise in user numbers, as well as the convergence of information and communications technologies, also make systems more vulnerable. It is therefore important to understand efficient data hiding scheme that use steganography and cryptography technique.

The rest of the paper is structured as follows: Section two discusses the background of the study, Section three reviews related literature on data hiding scheme, steganography and cryptography techniques. Section four presents the research gaps/findings from the literature and finally Section five concludes the study with recommendation for policies, for practices and direction of future works.

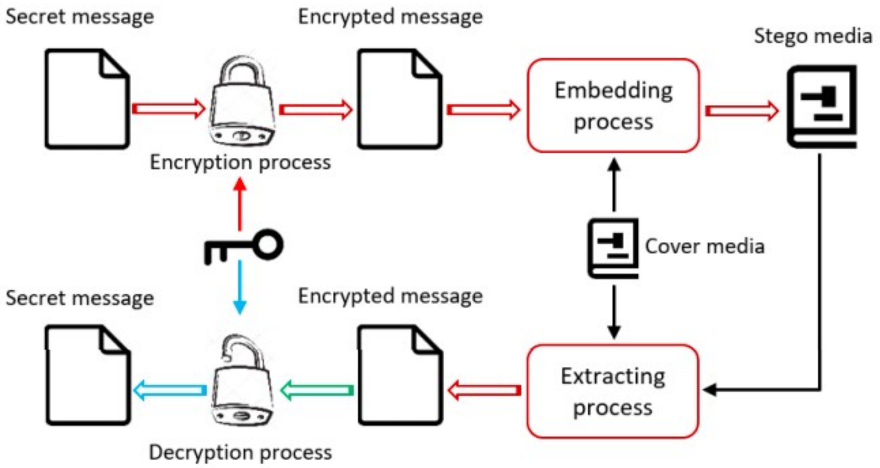


Fig 1: Combining Steganography & Cryptography
Source: Mustafa Sabah Taha et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 518 052003
https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf

This study is to understand the efficient data hiding scheme using steganography and cryptography technique. Due to advances in computer performance and communication technologies, Internet usage has grown significantly in recent years. In order to communicate and receive information on the Internet, digital elements including image, video, movie, and audio files are typically employed (Kim et al., 2019). The establishment of a secure communication between two communicating parties is becoming a difficult problem due to the likelihood of attacks and other unintentional changes during an active communication over an unsecured network (Taha et al., 2019). However, the security of secret information can be secured using either cryptography or steganography. Attackers have improved their cyberattack capabilities, yet the majority of the world's critical infrastructure systems continue to use outdated technology that are susceptible to low-tech cyberattacks (Da & Zekeriya Gündüz, 2019).

In recent years, cyber-attacks targeting critical infrastructures such as water plants, gas plants, power plants, and transportation systems are professional and specially designed. In modern technology is almost inspirable from our daily life. Since its beginning in the 1990s, the internet has a vast electronic network (Sharma, 2016). This network consist of millions of devices which is hyper-connected to each other. With the advancement of technology in last few decades in each sector, cybercrime is also increases day by day using these technologies. Cybercrime is a crime that involves in a computer and a network. Cyber criminals have become so smart in this 21st century, and working in collaborative manner making cybercrime a serious issues for all over the world. These types of people done several types of crime like financial crimes, cyber pornography, online gambling, cyber defamation, virus/warm, web jacking, email spoofing, data diddling etc.

It is necessary to fight back to these types of culprits to save the people, so there are several organizations who are continuously working to prevent cybercrime like Government agencies, Police department, Cybercrime bureau etc. Cyber security means protecting information and information systems (networks, computers, data bases, data centers and applications) with technological security. The increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions, the protection of personal and sensitive data have assumed paramount importance (Sharma, 2016). The economic growth of any nation and its internal security depends on how well is its cyberspace secured and protected. To solve these problems, the efficiency of data-hiding scheme, steganography, cryptographic techniques and techniques are used to prevent illegal use of information. Two different techniques use for protecting the authenticity and confidentiality of data are steganography and cryptography (Joseph & Sundaram, 2011; Saleh, 2016). Data protection has become increasingly important to scholars and business professionals as increased Internet usage and the abundance of digital data public and private (Djebbar et al., 2012).

Numerous applications that utilize cryptographic techniques to provide data security have been created. Cryptography is a key component of secure information and communications systems. Both the secrecy and the integrity of data can be effectively protected with cryptography, and each of these applications has its advantages. But the broad application of cryptography presents a number of significant questions. Governments are charged with a variety of duties, some of which are directly related to the use of cryptography, such as safeguarding citizens' right to privacy, facilitating the security of information and communications systems, fostering economic growth by, in part, promoting electronic commerce and preserving public safety

Also generating revenue to fund their operations, and enabling the enforcement of laws and the preservation of national security. While there are legitimate governmental, economic, and private needs and uses for cryptography, it can also be used for illicit purposes by people or organizations, which can have a negative impact on privacy, public safety, and national security. The task of creating balanced policies to address these concerns is one that governments, business, and the general public must participate.

2. RELATED LITERATURE

This section examines related literature on data hiding scheme, steganography and cryptography techniques. A literature review is a thorough summary of earlier studies on a subject. The literature review examines scholarly books, journals, and other sources that are pertinent to a particular field of study. This prior research should be listed, described, summed up, impartially evaluated, and clarified in the review. It need to provide a theoretical framework for the study and assist the author in defining its scope. By acknowledging the contributions of earlier researchers, the literature review reassures the reader that the work has been thoughtfully conceived.

A literature review's objectives are to: 1. Provide background information on the subject, 2. Determine areas of prior research to avoid duplication and to properly credit other scholars, 3. Recognize contradictions, such as gaps in the literature, inconsistencies between studies, and unanswered questions from other studies, 4. Determine the need for more research to justify the research, 5. Determine the connection between the works and their impact on the subject and other works, 6. Put your own findings in the context of the existing literature and argue why more research is necessary.

Data hiding scheme

Data hiding scheme is a technique that hides the existence of secret data from malicious attackers (Kim et al., 2019). Therefore, malicious attackers cannot know the existence of secret data in digital contents. Data hiding or digital watermarking techniques are used steadily for complete digital information and copyright protection. Watermarking embeds a watermark on digital contents to prevent copyright problems. To transfer sensitive data from one host to another, data embedding schemes are common worldwide. It moves readily to concerned hosts while maintaining the privacy of the original data. This strategy is broken down into two sections, namely: To protect privacy, data concealing may hide a hidden message or data with a cover file. Data concealing method assisted by cryptography to encode and decode the original data. Typically, a cryptography solution is employed to give original data more privacy. This method's primary goal is to send the original file or message to the target location while maintaining strict privacy and using less data to transport data efficiently.

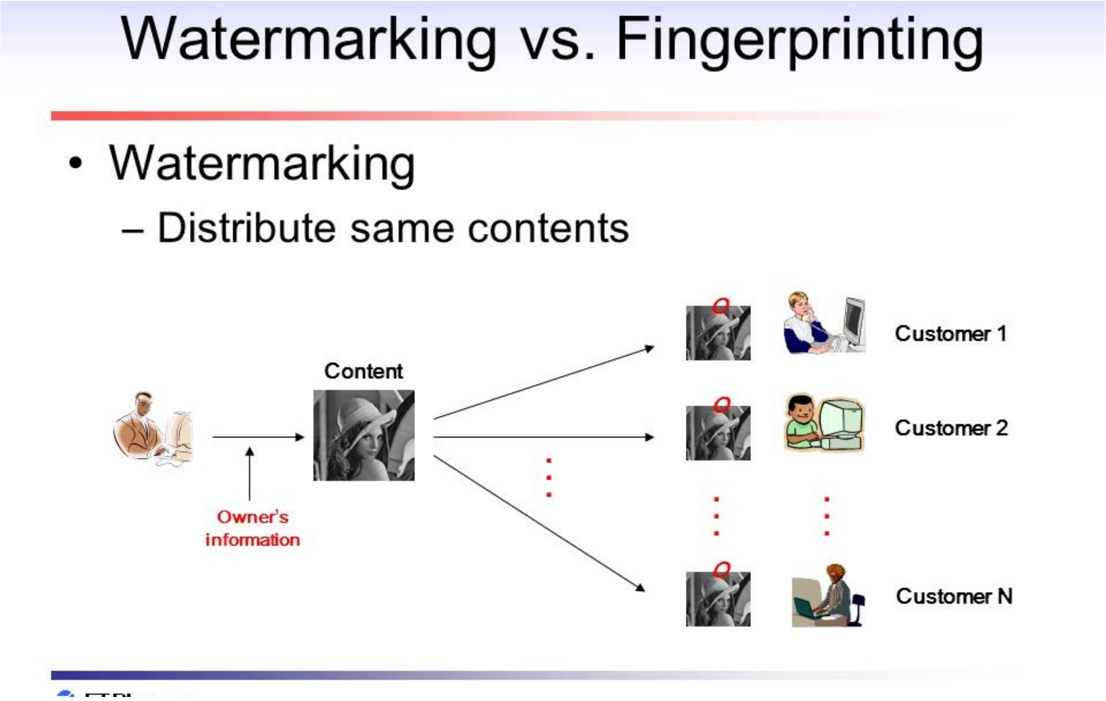
Steganography techniques

Increasing proliferation of digital data consumption in many practical applications require new and efficient methods to maintain its security are urgently needed (Djebbar et al., 2012). Steganographic techniques can be used to, at least in part, achieve effective secrecy. There have been some creative and adaptable audio steganographic methods presented. The purpose of steganographic systems is to find a reliable and safe method of hiding a large amount of hidden data (Djebbar et al., 2012). There are various prominent source of data hiding across novel telecommunication technologies such as covered voice-over-IP, audio conferencing, etc.

The multitude of steganographic criteria has led to a great diversity in these system design techniques. In this paper, we review current digital audio steganographic techniques and we evaluate their performance based on robustness, security and hiding capacity indicators. Another contribution of this paper is the provision of a robustness-based classification of steganographic models depending on their occurrence in the embedding process. A survey of major trends of audio steganography applications is also discussed in literature.

Watermarking and fingerprinting

Among the technologies related to steganography are **Watermarking and fingerprinting** used for intellectual property protection (Morkel et al., 2005). A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark is hidden in the host data in such a way that it cannot be removed without demeaning the host medium. Though this method keeps the data accessible, but it is permanently marked. The hidden information in a watermarked object is a signature referring to the origin or true ownership of the data in order to ensure copyright protection. In the case of fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the intellectual property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups.



Watermarking vs. Fingerprinting

- Watermarking
  - Distribute same contents

Content

Owner's information

Customer 1

Customer 2

Customer N

Fig 2: Watermarking & Fingerprinting
Source: https://slideplayer.com/slide/4736517/

Cryptography Techniques

A combination of steganography and cryptography empower individuals to impart without conceivable meddlers not withstanding knowing there is a type of correspondence in any case (Kulkarni et al., 2016). Steganography differs from cryptography (Hamid & Ahmad, 2012). The goal of cryptography is to secure communications by changing the data into a form that an eavesdropper cannot understand.

Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is. In some cases, sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the best solution for secure communication; it is only part of the solution. Both sciences can be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well.

4. RESEARCH FINDINGS

Extent literature has proposed models and methods in this work allow for construction of effective mechanisms to protect cyber security in banking systems at the canonical, logical, and physical levels of their representation, limiting access and admission to the content of their data to only those with appropriate user authority, and establishing rules for user interaction with information resources based on optimal, requirements-consistent criteria. This provides the most significant possible architecture for easy access and the safest means to protect their data from various threats.

Studies have been conducted aimed at reviewing the several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were presented as well (Taha et al., 2019). Findings show that steganography and cryptography are both known to fall short of providing full information security, combining the two can result in a stronger and more dependable system [45]. Combining these tactics can assure increased secret information protection and will satisfy the security and robustness criteria for sending crucial information via open channels. The growth in the amount of data being exchanged through the Internet has increased awareness of information security. Exploiting the benefits of steganographic and cryptographic techniques by mer ging them together into a hybrid methodology is one of the potential solutions.

Almuhammadi et al. conducted a comparison between steganography and cryptography [66]. They looked at various approaches to integrating steganographic and cryptographic methods into a single system. Additionally, they categorize these techniques and contrast them based on the encryption algorithms used, the steganographic approach employed, and the file type used as a cover. In light of this, they came to the conclusion that methods that begin with cryptography are more prevalent than those that begin with steganography and offer higher security with less encrypted data exposure. Steganographic techniques' only benefit was that they allowed for more hidden information to be stored.

5. RECOMMENDATION FOR POLICIES AND PRACTICES

Recommendation for Policy

The need for a standard on cryptography policy. Cryptography is a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use. It is one of the technological means to provide security for data on information and communications systems as well as trust in economic and social activities that rely on such data (OECO, 2022).

Recommendation for practice

Cryptography can be an effective tool for the secure use of information technology by ensuring confidentiality, integrity and availability of data and by providing authentication and non-communications networks and systems; repudiation mechanisms for that data, it is an important component of secure information

6. DIRECTION OF FUTURE WORKS

Future research will how to secure cybersecurity issues as digitalization become critical. The storage of big data will rely on technologies such as the cloud. Risks and threats should be contextualized, and a realistic evaluation of what may go wrong should be part of security management.

7. CONCLUSION

The main aim of this study is to understand efficient data hiding scheme using steganography and cryptography techniques. Advantages of efficient of these concepts can enhance cyber security by 1. Improve security of cyberspace 2. Increase in cyber defense 3. Increase in cyber speed 4. Protecting company data and information 5. Protects systems and computers against virus, worms, malware and spyware 6. Protects individual private information 7. Protects networks and resources 8. Fight against computer hackers and identity theft 9. Minimizes computer freezing and crashes. 10. Gives privacy to users. The act of secret writing through the encoding and decoding of encoded messages is known as cryptography. Steganography, on the other hand, refers to the ways of concealing a secret message into a cover message in such a way that its existence is completely hidden. Despite conducting a comparison study between the sciences of cryptography and steganography, the authors are unable to guarantee that steganography can be used as a substitute for cryptography. The system will become open to outside interference if only one of these methods is used. In order to increase security and robustness, steganography and cryptography are combined for efficiency.

Relevant literature was reviewed on cryptography and steganography techniques used to protect data over network. Recommendation for policy and practice as well as direction for future works were presented.

REFERENCES

1. Da, R., & Zekeriya Gündüz, M. (2019). Analysis of Cyber-Attacks in IoT-based Critical Infrastructures. *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE Da¸sDa¸s et Al*, *8*(4), 122–133.
2. Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, AndMusic Processing*, 1–16.
3. Hamid, N., & Ahmad, R. B. (2012). Image Steganography Techniques : An Overview Image. *International Journal of Computer Science and Security (IJCSS)*, *6*(3), 168–187.
4. Horng, J. H., Xu, S., Chang, C. C., & Chang, C. C. (2020). An efficient data-hiding scheme based on multidimensional mini-SuDoKu. *Sensors (Switzerland)*, *20*(9), 1–19. https://doi.org/10.3390/s20092739
5. Joseph, A., & Sundaram, V. (2011). *Cryptography and steganography–A survey*.
6. Kim, P., Yoon, E., Ryu, K., & Jung, K. (2019). Data-Hiding Scheme Using Multidirectional Pixel-Value Differencing on Colour Images. *Hindawi Security and Communication Networks*, *2019*.
7. Kulkarni, M., Phatak, M., Rathod, U., Prajapati, S., & Mujgond, S. (2016). Efficient data hiding scheme using audio steganography. *International Research Journal of Engineering and Technology*, *3*(3), 1701–1706.
8. Morkel, T., Eloff, J. H. P., & Olivier, M. S. (2005). An overview of image steganography. *ISSA*, *1*(2), 1–11.
9. Mustafa Sabah Taha et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 518 052003 https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf
10. OECO. (2022). *CECD, Recommendation of the Council concerning Guidelines for Cryptography Policy*.
11. Saleh, M. E. (2016). Data Security Using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Applications*, *7*(6), 390–397.
12. Sharma, P. (2016). *Cybercrime : Internal Security threat*. 14–17.
13. Taha, M. S., Shafry, M., & Rahim, M. (2019). Combination of Steganography and Cryptography : A short Survey. *IOP Conference Series: Materials Science and Engineering PAPER*. https://doi.org/10.1088/1757-899X/518/5/052003
14. Watermarking and Fingerprinting - . https://slideplayer.com/slide/4736517/