JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

TITLE: IMAGE STEGANOGRAPHY USING THE ADVANCED ENCRYPTION STANDARD (AES) IN HEALTHCARE SYSTEM

CONCEPT PAPER BY:

DENVER WEKESA – I132/G/1202/21
ALEX OUMA BARASA – I132/G/1652/21

INTRODUCTION

In health industry; storing, sharing and management of patients' information has been influenced by the current technology. That is, medical centers employ electronical means to support their mode of service in order to deliver quality health services. The importance of the patients' records cannot be overemphasized as it contributes to when, where, how, and how lives can be saved. Healthcare organizations have encountered no less than one data breach, costing more million on average per organization. Medical records attract high degree of importance to hoodlums compare to Mastercard information because they infer more cash base on the fact that bank cards can rapidly be crossed out in order to prevent the potential harm while medical data cannot be so easily destroyed.

BACKGROUND INFORMATION

we are in an era where technology usage in healthcare industry is growing more popular than a few years ago. This means that there is more need to protect our digital asserts from unauthorized access. The main aim is to secure the medical records by ensuring safe communication between the sender and the receiver by adding multiple layers of security. This project is a combined approach of both encryption and steganography techniques to give security the utmost importance required. Encryption is divided into two types that is symmetric encryption and asymmetric encryption. In our project we are basing our research on symmetric encryption which is Advanced Encryption Standard (AES). Symmetric encryption achieves this by enabling the original content to be shown only after the correct key is used to decrypt the information. It prevents interception and theft of private information over networks. Encryption and steganography guarantee the confidentiality, integrity, identifiability, and non-repudiation of information. In the sender, only the authorized person can send the secret image to the receiver. In the first stage, an image steganography system is processed using confidential medical information which are hidden under the cover images. The encryption method used is based on Random Number Generator and the pixel indicator, in other words, by moving the position of the pixel in the image to encrypt the information on the transmitting side. Whereas on the receiver side, this project proposes a method to authenticate the receiver by incorporating Email Authentication and OTP Verification to decrypt the encrypted information.

PROBLEM STATEMENT

As the volume of medical information stored electronically increases, so do the need to enhance how it is secured. Sensitive patient data, such as medical records, diagnostic images, and treatment plans, is vulnerable to unauthorized access and disclosure. The inaccessibility to patient record at the ideal time can prompt death toll and also well degrade the level of health care services rendered by the medical professionals. This project therefore presents the combination of AES and LSB to improve security measures applied on medical data.

OBJECTIVES

Main Objective:

- To develop a secure and efficient steganographic system based on the Advanced Encryption Standard (AES) for protecting sensitive patient data in the healthcare sector.

Specific Objectives:

1. To design and implement a robust AES-based steganography algorithm.
2. To evaluate the performance of the steganographic system.
3. To address scalability and efficiency in relation to data security.
4. To ensure compliance with data privacy in relation to Informational Technology industry regulations.
5. To integrate the steganography system into a healthcare environment as a method for efficient data storage and transit.

Research Questions

i. What are the main issues with hiding data securely?
ii. How can steganography help keep data safe?
iii. What are the common steganography methods and how do they differ in security and capacity?
iv. How does encryption make steganography systems safer?
v. How can we protect against modern threats to secure data hiding systems?
vi. Where can we use secure data hiding systems using steganography?
vii. What factors affect the balance between hidden data amount, security, and quality in steganography for different media types?

Significance of the Study

In healthcare sector, it's important to keep patient information safe and private. If we use image steganography, we are going to hide important patient data, like medical records and test results, inside pictures. This makes it extra difficult for unauthorized people to get access to the information. Healthcare providers can use this technique to make sure that private data stays safe when it's shared or stored on computers. This is really important for following privacy rules and keeping patients' trust. It also helps to stop hackers from getting hold of the information, which could be really serious for both patients and healthcare organizations.

Our research project also aims at Securing Online Doctor-Patient Communication**:** As more people use telemedicine (online healthcare services), it’s important to keep their medical information safe. Steganography hides sensitive data, like test results, inside images when sent over the internet, making it harder for hackers to steal during online doctor visits

Scope

TASK	DURATION				
	OCTOBER	NOVEMBER	DECEMBER	JANUARY	FEBRUARY
Concept paper.	▨				
Project proposal		▨			
Proposal defense		▨			
System design			▨		
System implementation			▨	▨	▨
Testing and training.				▨	▨
Documentation	■	■ =	■	■	■

Definition of terms:

Encryption is the process of making information only readable to certain receivers and incomprehensible to other users.

Symmetric encryption which is also called shared key cryptography, uses the same key to encrypt and decrypt data. That is, the sender and receiver must use the same key.

Asymmetric encryption uses two different keys: a public key and a private key. A public key and a private key are a pair. If a public key is used to encrypt data, only the corresponding private key can be used to decrypt the data.

Steganography is derived from two Greek words firstly Steganos (covered or concealed) and Graphy (Writing) that means “covered writing” which basically mean to hide data and information into a plain sight.

Covered Image: Real image acting as a carrier for the hidden file

Hackers: are individuals or groups who try to gain unauthorized access to computer systems, networks, or data

Concealed Data: Hidden data

REFERENCES

Hambouz A et al. 2019 Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques Proc. 2nd Int. Conf. on new Trends in Computing Sciences, Amman, Jordan, pp. 1-6.

UIC, (2017). Why Data Security is The Biggest Concern of Health Care. Retrieved from: http://healthinformatics.uic.edu/resources/articles/why-data-security-is-the-biggest-concern-of-health-care/ Retrieved date: 17th July, 2017.

American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN: 2320-0936 Volume-02, Issue-11, pp-122-128

(Kulecho & Barasa, n.d.)