­­­­­VISVESVARAYA TECHNOLOGICAL UNIVERSITY

“JNANA SANGAMA”, BELGAUM – 590018, KARNATAKA



A Project Synopsis on

“StegMate – Android-based Steganography Application”

Submitted in Partial Fulfilment of the Requirement of the Award of the Degree of

Bachelor of Engineering in Computer Science and Engineering

Submitted by

RAJEEV LAXMANRAO MAHENDRAKAR [4UB20CS034]

S. NETRA [4UB20CS035]

SAHANA S.N [4UB20CS036]

SANKETH KUMAR [4UB20CS037]

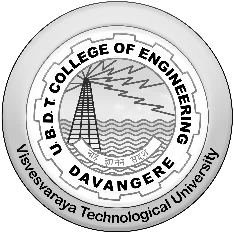
Under the Guidance of

Dr. Shreedhara K. S.

Chairman and HOD

DOS in Computer Science & Engineering

UBDTCE



­­

DEPARTMENT OF STUDIES IN COMPUTER SCIENCE & ENGINEERING

University B.D.T. College of Engineering, Davanagere – 577 004

VISION:

To be a centre of excellence in Education and Research in the field of Computer Science and Engineering by empowering the students to be highly competent, technologically proficient, self-motivated, innovative professionals, entrepreneurs and responsible global citizens possessing human values to meet the global challenges.

MISSION:

M1: To impact the students with strong fundamental concepts, analytical capability, and problem-solving skills, thereby enhancing the employability skills required for the industries.  
M2: To provide a conducive teaching learning, and research environment through faculty training, self-learning and sound academic practices to carry out research with reputed research institutes and industries.  
M3: To train the students to become the most sought-after professionals by providing them the opportunities to promote organizational and leadership skills in students through various extracurricular and co-curricular events.  
M4: To include the qualities of leadership and entrepreneurship with good human values and professional ethics to become good citizens and serve society.

ABSTRACT:

In today's society, the security of our personal information is a major concern. With the increasing use of technology in our daily lives, we are constantly sharing and using data that may not be entirely private. Hackers and scammers are always on the lookout for vulnerabilities in the network, making it difficult to ensure that our data is secure. Despite the many security measures in place, they are often not up to date and cannot keep up with the speed at which the network is growing. This puts many applications that require security at risk. To address this issue, we propose to develop more efficient techniques that can prevent data leaks and provide better data security. Our project aims to deliver solutions to the current challenges faced by users in terms of data security. We will work towards bridging the gap between the existing security measures and the current network requirements. By implementing advanced algorithms and techniques, we hope to provide better protection for personal data and ensure that it remains secure.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Chapter 1** | **INTRODUCTION**   * 1. PROBLEM STATEMENT   2. EXISTING SYSTEM   3. DISADVANTAGES OF THE EXISTING SYSTEM   4. PROPOSED SYSTEM |  |
| **Chapter 2** | **LITERATURE SURVEY** |  |
| **Chapter 3** | **SYSTEM REQUIREMENTS AND SPECIFICATIONS**  3.1 FUNCTIONAL REQUIREMENTS  3.2 NON-FUNCTIONAL REQUIREMENTS  3.3 HARDWARE AND SOFTWARE REQUIREMENTS |  |
| **Chapter 4** | **SYSTEM DESIGN AND ARCHITECTURE**  4.1 USE CASE DIAGRAM  4.2 SYSTEM FLOW DIAGRAM |  |
| **Chapter 5** | **METHODOLOGY**  5.1 ANDROID STUDIO  5.2 |  |
| **BIBLIOGRAPHY** | |  |

**CHAPTER 1**

**INTRODUCTION**

In today's world, we can accomplish various tasks with just a single click, thanks to the advancements in technology. People use their smartphones for various day-to-day tasks and share different media with the world. However, with these new revolutions, the need for data security has also increased. Cryptography and Steganography are two of the main techniques that offer this security[2]. Cryptography involves encrypting the data to make it unreadable, while Steganography is used to conceal the data into a cover file, hiding its existence. Various existing systems provide different Steganography-based applications, each implemented with different algorithms for different uses. These systems use different types of cover media to conceal data, and the data to be hidden varies from technique to technique. Some of the existing applications that help in securing data through Steganography are Stego App[2], MobiStego, MoBiSiS, and Smart Steg[3].

Steganography is a fascinating process that involves hiding secret information within an unsuspecting graphic. The word "steganos" comes from the Greek language, meaning "hidden" or "covered", while "graph" means "to write". Although Steganography techniques are advantageous to use, they have a few limitations. Our project introduces an Android application called "StegMate" that utilizes various types of steganography, such as text, video, audio, and network, to offer a more comprehensive approach to data security. The application ensures that any confidential message is only accessible to its intended recipients.

* 1. **Problem Statement**

The objective is to encode various types of secret media, such as images, text, and audio, into a cover file that can be an image, audio, or video. The produced stego-media, which is a media file with a secret message embedded within, can be shared with others. The recipients should be able to decode any of the stego-media that is shared with them. The system aims to reduce the load and increase efficiency during encoding/decoding, as well as reduce the time required to generate the stego-media. Additionally, it should be adaptable and integrated with new and emerging technologies.

The project's main objective is to develop an optimal technique for generating embedded media that can adapt to all types of extensions.

* 1. **Existing System**

In today's world, data security is of utmost importance. Many contenders, such as WhatsApp, fulfil this need by providing end-to-end encryption for all messages sent. Additionally, WhatsApp offers a feature called "once-view" where media can be viewed only once before disappearing. The SmartSteg Application uses the BMP image format, which is lossless, and the LSB algorithm for encryption[3]. Another application uses the RSA Algorithm and LSB Insertion to achieve Image Steganography[4]. The Stego App allows for embedding both text and images within an image[2]. Some applications also reduce the size of the stego-image to be MMS compatible, making it easier to share[1].

* 1. **Disadvantages of Existing System**

It is worth noting that while there is a systematic approach to embedding data into images, many applications have limited functionality that is restricted to their app. For instance, the widely used LSB insertion method only supports embedding into images and does not support multiple extension types. Additionally, some applications are outdated and do not support current image specifications, limiting their use to images with lower size and encoding. As a result, the usage of these apps has significantly decreased, and the current image-embedding apps are not multi-platformed.

* 1. **Proposed System**

Our proposed technique aims to provide users with a seamless way to embed various types of media, such as text, images, and audio, into a cover file. This cover file can support any extension for images or audio, making it a versatile solution for users. By reducing system resource consumption, we aim to increase the efficiency of the application, allowing users to perform tasks faster and more effectively. To achieve this, we plan to incorporate a mechanism for file upload and live media capture, enabling users to easily add new content to their cover files. Additionally, we will support file sharing, allowing users to share their cover files with others. To ensure the security of the application, we will implement robust security measures that prevent unauthorized access. This will ensure that only the user can access the application and their cover file, providing peace of mind and security.

**CHAPTER 2**

**LITERATURE SURVEY**

Data security is a very important aspect in today's world. Whilst all the systems are getting interconnected, securing the shared data is also important. There exist various challenges in the transmission of data. The term security has a very vast explanation.

Intellipaat[5] defines it as the protections put in place to secure databases, websites, and computers against unwanted access. This procedure also includes safeguards against data loss or corruption. Small firms and large enterprises should implement protection measures to secure data. Failure to have an effective information security plan in place can have severe repercussions for companies. According to the [*Economist*](https://www.economist.com/)*,* we are currently living in the “zettabyte age.” For the amount of traffic being generated, the most suitable step is to manage and safeguard the transfer of sensitive or personal information at every known location. Both proactive enterprises and global regulators are progressing significantly.

IBM[6] states that Data security is the practice of protecting digital information from unauthorized access, corruption or theft throughout its entire lifecycle. It’s a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures. Data security is the practice of protecting digital information from unauthorized access, corruption or theft throughout its entire lifecycle. It’s a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

Medium[7] - In the current digital era, data privacy and security have emerged as two pressing challenges. Data privacy and security are getting more complicated and contentious as more and more personal data is being gathered and analyzed. Personal data collection and storage have become simpler thanks to the digital age, but data theft has also become simpler for cyber criminals. Personal data is being gathered and processed at a rate that has never been seen before as our lives become more and more digital. Organizations are gathering a ton of personal information about people from social media platforms and e-commerce sites to healthcare providers and financial institutions. Although this information can be extremely useful for research, marketing, and other purposes, it also poses serious hazards to the security and privacy of the people who use it.

The New York Times[8] – Privacy can never be guaranteed with absolute certainty. The risks should always be minimized, and balanced against the benefits of the innovations that may arise from increased data availability. A better program would target aid to business sectors and geographies that most need help, using real-time data from the businesses themselves. This data already exists, but only behind company walls. It should be anonymized as carefully as possible and assembled for public use so that local policymakers and entrepreneurs can direct the relief to those who need it most.

The Journalist’s Resource[9] – On your smartphone, you’re not much more than a data machine, generating reams of valuable information that tech companies can mine for insights, sell to advertisers and use to optimize their products. But it’s easy to forget these [risks to personal privacy](https://live-journalists-resource.pantheonsite.io/studies/society/internet/the-state-of-internet-privacy-in-2013-research-roundup) and [security](https://live-journalists-resource.pantheonsite.io/studies/society/internet/unique-crowd-privacy-bounds-human-mobility) while tapping out messages to friends or scrolling endlessly through the web. The distraction machines at our fingertips ask for access and we give it up quickly, hastily agreeing to unread privacy policies and terms of service in exchange for a fresh jolt of content.

**CHAPTER 3**

**SYSTEM REQUIREMENTS AND SPECIFICATION**

**CHAPTER 4**

**SYSTEM DESIGN AND ARCHITECTURE**

**CHAPTER 5**

**METHODOLOGY**

Android is one of the most widely used mobile operating systems in the world. With its user-friendly interface, customizable features, and open-source platform, it has become a popular choice for mobile app development. Android app development has several advantages over other platforms. For starters, Android has a vast user base, which means that there is a high demand for Android apps. Additionally, Android apps can be developed using a wide range of programming languages, including Java, Kotlin, and C++. This offers developers the flexibility to choose the language that they are most comfortable with. Furthermore, Android provides a comprehensive set of tools and libraries that make the app development process more efficient. Overall, Android app development is an excellent choice for building robust, scalable, and user-friendly mobile applications.

Our project focuses on identifying different existing applications, testing them, and building more efficient, bug-free software that can be incorporated into many different industrial solutions.

OBJECTIVES:

* To learn about the different algorithms used in the process of Steganography.
* Discover and test the existing Steganography Applications and learn the technologies behind them.
* Identify the different Algorithms used for it.
* Implement our own Steganography Application using the learned techniques.

TECHNOLOGIES USED:

OS: Android

Programming Language: XML, Java

Algorithms Used: RSA, DES, AES

DIAGRAM:

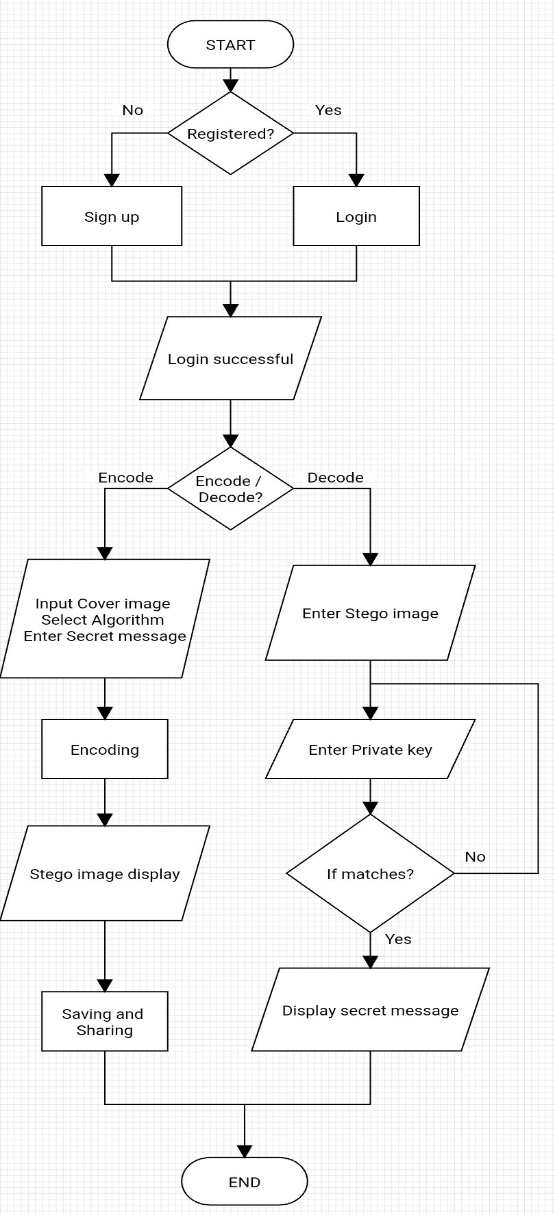


Fig 1: Flowchart of Application working

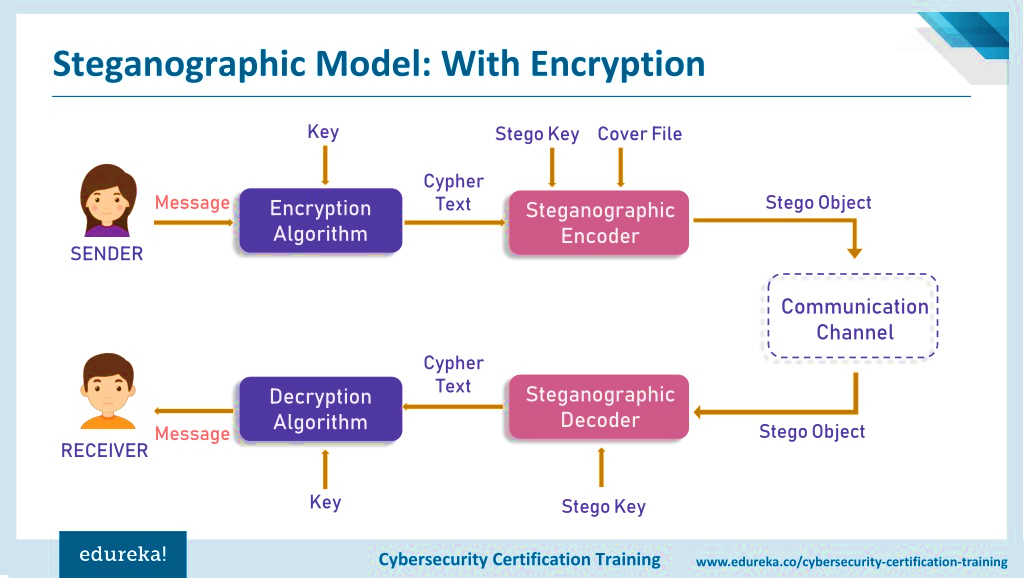


Fig 2: Process of Steganography

EXPECTED OUTCOME:

* Android Application with User Interaction – Registration and Login.
* It also includes the encoding and Decoding of Secret messages within Images.
* Sharing of the images is also included.

**BIBLIOGRAPHY**

[1] Zavrak, Sultan, Seyhmus Yilmaz, and Huseyin Bodur. "An Implementation of Android-based Steganography Application." International Journal of Computer Science and Information Security 13.12 (2015): 73.

[2] Ullah, Azmat, and Mohsin Ijaz. "Stego App: Android-based Image Steganography Application using LSB Algorithm." Int. Res. J. Eng. Technol 5.9 (2018): 862-865.

[3] Bucerzan, Dominic, Crina Ratiu, and Misu-Jan Manolescu. "SmartSteg: A new android-based steganography application." Int. J. Comput. Commun. Control 8.5 (2013): 681-688.

[4] Apau, Richard, and Clement Adomako. "Design of image steganography based on RSA algorithm and LSB insertion for Android smartphones." International Journal of Computer Applications 164.1 (2017): 0975-8887.

[5] [The Importance of Data Security in 2023 - Intellipaat](https://intellipaat.com/blog/importance-of-data-security/)

[6] [What is Data Security? Data Security Definition and Overview | IBM](https://www.ibm.com/topics/data-security)

[7] [Data Privacy and Security: The Importance of Protecting Personal Information in the Digital Age | by Ejike Uchenna Splendor | Medium](https://medium.com/@Splendor001/data-privacy-and-security-the-importance-of-protecting-personal-information-in-the-digital-age-d7e80627cb44)

[8] [Balancing Privacy With Data Sharing for the Public Good - The New York Times (nytimes.com)](https://www.nytimes.com/2021/02/19/business/privacy-open-data-public.html)

[9] [Data security: Research on privacy in the digital age (journalistsresource.org)](https://journalistsresource.org/economics/data-digital-privacy-cambridge-analytica/)