

Steganography of Encrypted Messages Inside Valid QR Code

Sindhu M

Assistant Professor

Abstract

Steganography is regarded as the primary defense mechanism in information security, as it conceals a secret message (payload) within an innocuous file (container) to transfer the payload without detection by an adversary. Steganographic systems utilize the container solely for the purpose of hiding the payload. In this paper, we introduce a steganographic system that employs the container not only to conceal the payload but also to provide misleading information to the adversary. To accomplish this objective, we utilize a quick response (QR) code as the container. The QR codes produced by our proposed system can convey their standard message alongside the payload. While anyone can access the message, the payload can only be retrieved using a secret key. The message and the payload are independent; that is, any message can be created irrespective of the payload and vice versa. We can leverage this by crafting a message that misleads the adversary. We evaluate the proposed system and demonstrate that the generated QR code is valid, meaning it is indistinguishable from a standard QR code, which renders it seemingly harmless and less vulnerable to adversarial attacks. Furthermore, it is space-efficient, possesses an acceptable degree of noise immunity, and is resistant to steganalysis attacks.

1. INTRODUCTION

1.1 PROJECT DESCRIPTION

Steganography is the practice of concealing secret information (payload) within an unassuming, ordinary, non-secret file (container). The term originates from the Greek words "stegos," meaning "cover," and "grafia," meaning "writing." Multimedia formats, such as images, are often chosen as containers for hiding the payload due to their ability to endure a certain level of distortion without compromising their quality.

Steganographic techniques are driven by the vulnerabilities present in encryption systems. These techniques allow for the transmission of secret information without detection, in contrast to encryption, which renders ciphertext identifiable and open to attacks. For instance, fully developed quantum computing could potentially be utilized to break and decode encrypted data. Additionally, certain governments impose regulations that restrict or entirely prohibit the use of cryptographic methods. This has prompted individuals and corporations to seek alternative solutions. Businesses are beginning to recognize the advantages of steganography; concealing information about new products within an innocuous family photograph is less likely to raise suspicion than sending an encrypted file. It is advisable to encrypt the payload prior to embedding it in a container to benefit from the security offered by both steganography and cryptography. QR codes are two-dimensional barcodes that can be read by machines, specifically through cameras. They are capable of encoding various forms of information, including alphanumeric characters and control codes. Examples of information that can be embedded in QR codes include a phone number, a URL, and an ID. QR codes were first introduced by Denso-Wave, a Japanese company affiliated with Toyota, in 1994. Initially, QR codes served as a means to efficiently track vehicle components. From that point, their usage expanded globally, particularly within the marketing and business sectors. QR codes provide a convenient and user-friendly method for sharing information. All that is required is to take a picture of the QR code with a cellphone. They have achieved significant success in advertising and marketing industries, being ubiquitous from food labels to large advertising displays.

2. LITERATURE SURVEY

2.1 EXISTING AND PROPOSED SYSTEM

Cryptography was developed as a method to ensure the confidentiality of communication, and numerous techniques have been established to encrypt and decrypt data to maintain the secrecy of messages. However, it is occasionally insufficient to merely keep the contents of a message confidential; it may also be essential to conceal the very existence of the message. Cryptography is the discipline of safeguarding information during its transmission. The sender processes the information in such a manner that renders it unreadable. The resulting cipher text exhibits a uniform distribution, meaning the likelihood of a bit being '1' or '0' is 50%. Decryption can only be accomplished using a secret key. Regrettably, there are instances when merely securing information is inadequate, and it becomes imperative to obscure its existence.

LIMITATIONS OF EXISTING SYSTEM

- Occasionally, securing information is insufficient, and it is crucial to hide its existence.
- Only offers encrypting and decrypting capabilities.

PROPOSED SYSTEM

Steganography is both an art and a science focused on invisible communication. This is achieved by concealing information within other information, thereby obscuring the presence of the communicated data. Nearly all digital file formats can be utilized for steganography; however, those formats that exhibit a high level of redundancy are particularly advantageous. Redundancy refers to the bits within an object that offer a level of precision significantly exceeding what is necessary for the object's intended use and display. The redundant bits are those that can be modified without easily detectable changes. Image and audio files notably meet this criterion, while research has also identified additional file formats suitable for information concealment.

The proposed system comprises three modules: Admin, Manager, and Military. The Admin and Manager operate as web components, while the Military functions as the Android segment of the system. The Manager transmits messages to the Military based on state and location. To conceal the information, a QR code is generated once the message is dispatched, with the encrypted message embedded within the QR code and sent to the Military (Android). The Military officer logs in to receive the message, which is visible only once. The Military can view the QR code after entering the first password, at which point the encrypted message becomes accessible. The Military then employs a second password to decrypt the message. The Admin (web) has the capability to trace all messages sent by individual Managers.

ADVANTAGES OF PROPOSED SYSTEM

1. Enhanced error correction.
2. QR codes are scannable from any angle.
3. Compact printout size. QR codes are capable of storing messages in two dimensions, thereby optimizing space usage.
4. Significant data capacity. A QR code can encode up to 4,296 alphanumeric characters, 7,089 numeric characters, and 1,817 kanji characters.
5. Rapid scanning speed.

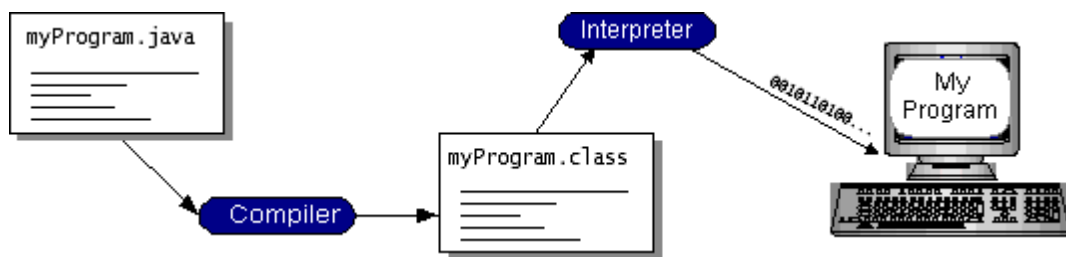
2.2 TOOL AND TECHNOLOGY USED

Java Technology

Java technology is both a programming language and a platform.

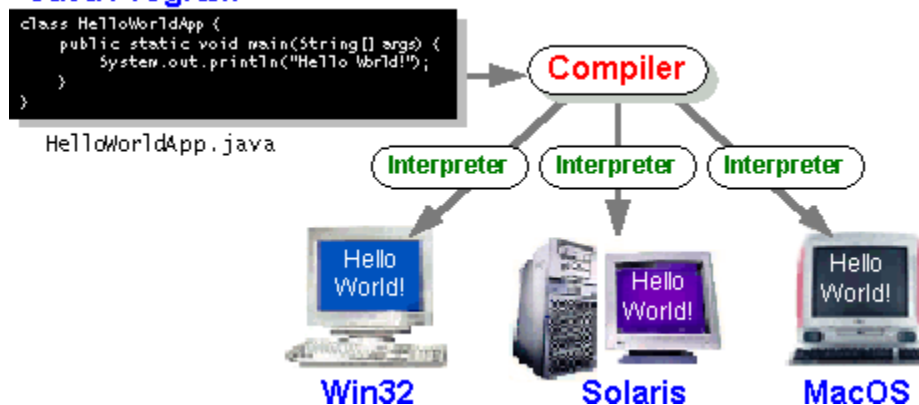
The Java Programming Language

In the majority of programming languages, a program is either compiled or interpreted to enable execution on a computer. However, the Java programming language is distinctive in that it involves both compilation and interpretation. Initially, the compiler translates a program into an intermediate language known as Java byte codes—these are platform-independent codes that the interpreter on the Java platform subsequently interprets. The interpreter processes and executes each Java byte code instruction on the computer. Compilation is performed only once, while interpretation takes place every time the program is run. The subsequent figure demonstrates this process.



Java byte codes can be regarded as the machine code instructions intended for the Java Virtual Machine (Java VM). Each Java interpreter, whether it is a development tool or a web browser capable of executing applets, serves as an implementation of the Java VM. The existence of Java byte codes facilitates the concept of 'write once, run anywhere.' You are able to compile your program into byte codes on any platform equipped with a Java compiler. Subsequently, these byte codes can be executed on any version of the Java VM. This implies that as long as a computer possesses a Java VM, the identical program developed in the Java programming language can operate on Windows 2000, a Solaris workstation, or an iMac.

Java Program



The Java Platform

A platform refers to the hardware or software environment in which a program operates. We have previously discussed several of the most widely used platforms, including Windows 2000, Linux, Solaris, and Mac OS. Generally, platforms can be characterized as a blend of the operating system and hardware. The Java platform is distinct from most other

platforms in that it is a software-only platform that operates on top of various hardware-based platforms.

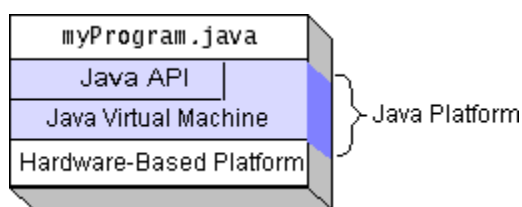
The Java platform consists of two main components:

- The Java Virtual Machine (Java VM)
- The Java Application Programming Interface (Java API)

You have already been introduced to the Java VM, which serves as the foundation for the Java platform and is adapted for use on different hardware-based platforms.

The Java API comprises a vast array of pre-built software components that offer numerous valuable features, including graphical user interface (GUI) widgets. The Java API is organized into libraries of related classes and interfaces, which are referred to as packages. The subsequent section, What Can Java Technology Do?, emphasizes the functionalities provided by some of the packages within the Java API.

The figure below illustrates a program executing on the Java platform. As depicted, the Java API and the virtual machine shield the program from the underlying hardware.



Native code refers to code that, once compiled, operates on a specific hardware platform. In contrast, the Java platform, which is designed to be platform-independent, may exhibit slightly slower performance compared to native code. Nevertheless, advanced compilers, optimized interpreters, and just-in-time bytecode compilers can enhance performance to levels comparable to native code while maintaining portability.

The Java platform offers the following features:

- **The essentials:** Objects, strings, threads, numbers, input and output, data structures, system properties, date and time, among others.
- **Applets:** A collection of conventions utilized by applets.
- **Networking:** Includes URLs, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) sockets, and IP (Internet Protocol) addresses.
- **Internationalization:** Provides assistance for developing programs that can be localized for users globally. Programs can automatically adjust to specific locales and present information in the correct language.
- **Security:** Encompasses both low-level and high-level security measures, including electronic signatures, management of public and private keys, access control, and certificates.
- **Software components:** Referred to as JavaBeans™, these can integrate into existing component architectures.
- **Object serialization:** Facilitates lightweight persistence and communication through Remote Method Invocation (RMI).

Java Database Connectivity (JDBC™): Ensures consistent access to a diverse array of relational databases.

Android is a mobile operating system that is based on a modified version of the Linux kernel along with other open-source software, specifically designed for touchscreen mobile devices like smartphones and tablets.

Android is developed by a group of developers referred to as the Open Handset Alliance, with commercial sponsorship from Google. It was first introduced in November 2007, and the initial commercial Android device, the HTC Dream, was released in September 2008.

This operating system is free and open-source; its source code is recognized as the Android Open Source Project (AOSP), which is mainly licensed under the Apache License. Nevertheless, the majority of Android devices come with additional proprietary software pre-installed, most notably Google Mobile Services (GMS), which encompasses essential applications such as Google Chrome, the digital distribution platform Google Play, and the associated Google Play Services development platform.

HTML Hypertext Markup Language:

HTML serves as the standard markup language utilized for the development of web pages and web applications. Together with Cascading Style Sheets (CSS) and JavaScript, it constitutes a triad of fundamental technologies for the World Wide Web. Web browsers obtain HTML documents from a web server or local storage and render them into multimedia web pages. HTML semantically describes the structure of a web page and initially included indications for the document's appearance. HTML elements act as the foundational components of HTML pages. Through HTML constructs, images and other objects, including interactive forms, can be integrated into the rendered page. It offers a method to create structured documents by indicating structural semantics for text, such as headings, paragraphs, lists, links, quotes, and other elements. HTML elements are defined by tags, which are written using angle brackets. Tags like `` and `<input />` directly introduce content into the page. Other tags, such as `<p>...</p>`, enclose and provide context for document text and may contain additional tags as sub-elements. While browsers do not display the HTML tags, they utilize them to interpret the content of the page. HTML also allows for the embedding of programs written in a scripting language like JavaScript, which can influence the behavior and content of web pages.

CSS Cascading Style Sheets:

CSS is a style sheet language utilized for defining the presentation of a document that is composed in a markup language. While it is predominantly employed to establish the visual aesthetics of web pages and user interfaces created in HTML and XHTML, this language can also be utilized for any XML document, which includes plain XML, SVG, and XUL, and is relevant for rendering in speech or on various media. Together with HTML and JavaScript, CSS serves as a fundamental technology leveraged by the majority of websites to develop visually appealing web pages, user interfaces for web applications, and user interfaces for numerous mobile applications. The primary purpose of CSS is to facilitate the separation of presentation from content, encompassing elements such as layout, colors, and fonts.

This separation enhances content accessibility, offers greater flexibility and control in defining presentation attributes, allows multiple HTML pages to share formatting by referencing the appropriate CSS in a distinct .css file, and minimizes complexity and redundancy in the structural content.

BOOTSTRAP

Bootstrap is a free and open-source front-end web framework designed for creating websites and web applications. It includes design templates based on HTML and CSS for typography, forms, buttons, navigation, and other interface components, along with optional JavaScript extensions. In contrast to many web frameworks, it focuses solely on front-end development. Bootstrap ranks as the second most-starred project on GitHub, boasting over 107,000 stars and 48,000 forks. Initially called Twitter Blueprint, Bootstrap was created by Mark Otto and Jacob Thornton at Twitter to promote consistency across internal tools. Prior to Bootstrap, various libraries were utilized for interface development, resulting in inconsistencies and a significant maintenance burden. As stated

by Twitter developer Mark Otto: “A super small group of developers and I got together to design and build a new internal tool and saw an opportunity to do something more.

Through this process, we recognized that we were creating something far more significant than just another internal tool. Months later, we produced an initial version of Bootstrap to document and disseminate common design patterns and assets within the organization. Following several months of development by a small team, numerous developers at Twitter started contributing to the project during Hack Week, a hackathon-style event for the Twitter development team. The project was renamed from Twitter Blueprint to Bootstrap and was launched as an open-source initiative on August 19, 2011. It has been continuously maintained by Mark Otto, Jacob Thornton, and a select group of core developers, along with a vast community of contributors. On January 31, 2012, Bootstrap 2 was launched, introducing a twelve-column responsive grid layout system, built-in support for Glyphicons, several new components, and modifications to many existing components. On August 19, 2013, Bootstrap 3 was released, which revamped components to adopt flat design and a mobile-first approach. On October 29, 2014, Mark Otto announced that Bootstrap 4 was under development. The first alpha version of Bootstrap 4 was made available on August 19, 2015. Bootstrap 3 is compatible with the latest versions of Google Chrome, Firefox, Internet Explorer, Opera, and Safari (with the exception of Windows). It also supports back to IE8 and the most recent Firefox Extended Support Release (ESR). Since version 2.0,

Bootstrap facilitates responsive web design. This indicates that the arrangement of web pages adapts dynamically, considering the specifications of the device being utilized (desktop, tablet, mobile phone). Beginning with version 3.0, Bootstrap embraced a mobile-first design approach, prioritizing responsive design by default. The alpha release of version 4.0 introduced support for Sass and flexbox. This involves installing and linking Bootstrap to the HTML page.

MySQL

MySQL is an open-source Relational Database Management System. It is known for being fast, reliable, and flexible. MySQL offers high performance and operates as a multi-threaded, multi-user Relational Database Management System. It ranks among the most widely used relational database management systems on the internet. The MySQL Database has emerged as the world's leading open-source database due to its free availability across nearly all platforms. MySQL can operate on UNIX, Windows, and Mac OS. It is favored for internet applications because of its speed and security. MySQL was designed to handle large data volumes at high speeds, addressing the limitations of previous solutions. While MySQL can be utilized for a variety of applications, it is predominantly employed for web applications on the internet.

2.3 HARDWARE SOFTWARE REQUIRMENTS

HARDWARE REQUIREMENTS:

- Processor - i3 or i4
- Speed - 1.1 Ghz
- RAM - 2GB
- Hard Disk - 20 GB

SOFTWARE REQUIREMENTS:

- Operating System : Windows
- Programming Language : JAVA/J2EE
- Storage :MySQL

- Browser :Google chrome, Mozilla Firefox
- front end :HTML,XML,JAVASCRIPT
- back end :Java

SOFTWARE REQUIREMENT SEFICATION

A software requirements specification (SRS) is a document that outlines the expected functionalities and performance of the software. It details the necessary features that the product must provide to meet the complete needs of all users, serving as a comprehensive specification and description of the software requirements essential for the successful development of the software system. These requirements may be categorized as functional or non-functional, depending on their nature. Understanding the interaction among various users is crucial to fully grasp their needs.

USERS

There are three Users Admin (web)

- Admin login
- Admin add managers
- Admin add military
- Admin add state
- Admin location
- Admin trace messages sent by individuals managers Manager(web)
- Manager login
- Manager select military officer
- Manger send message
- Manger generate QR code
- Manager view sent messages
- Manager logout

Military (android)

- Military login
- Military view message(visible only once)
- Military view QR CODE
- Military enters password
- Military gets encrypted message
- Military enter password
- Military decrypted message
- Military logouts

2.4 FUNCTIONAL REQUIREMENTS

A functional requirements document outlines the capabilities of a system or one of its subsystems. Its content is influenced by the software type, anticipated users, and the system environment in which the software operates. While functional user requirements may consist of broad statements regarding the system's intended functions, functional system requirements must provide a detailed description of the system's services. This represents the essential deliverable of the system, which can be considered its primary objective. In this context, a function is defined as a specification of the relationship between inputs and outputs. The requirements should clarify what constitutes system input and what the expected output is.

The functional requirements area

1. **Login:** Admin, manager, and military personnel can log in using their provided credentials.
2. **Add:** The admin has the capability to add managers, military personnel, and state locations.
3. **Trace messages:** The admin can trace messages sent by individuals.
4. **Message:** The manager can send messages and view the sent messages, which are encrypted in a QR code for security, ensuring that only authorized users can access them.
5. **QR Code:** Messages are concealed within a QR code for security, with the QR code password being valid for a single use only.
6. **Encrypt and Decrypt:** Each message sent from the manager to the military is encrypted in a QR code, and upon entering the password, the messages can be decrypted for the receiver to view.

2.5 NON FUNCTIONAL REQUIREMENTS

Non-functional requirements are constraints that must be followed during the development process. They restrict the resources that can be utilized and establish limits on various aspects of the software's quality. A crucial aspect of non-functional requirements is their verifiability. Verification is typically conducted by assessing different facets of the system and determining whether the results align with the specified requirements.

Non-functional requirements are categorized into several groups: The first category encompasses five quality attributes:

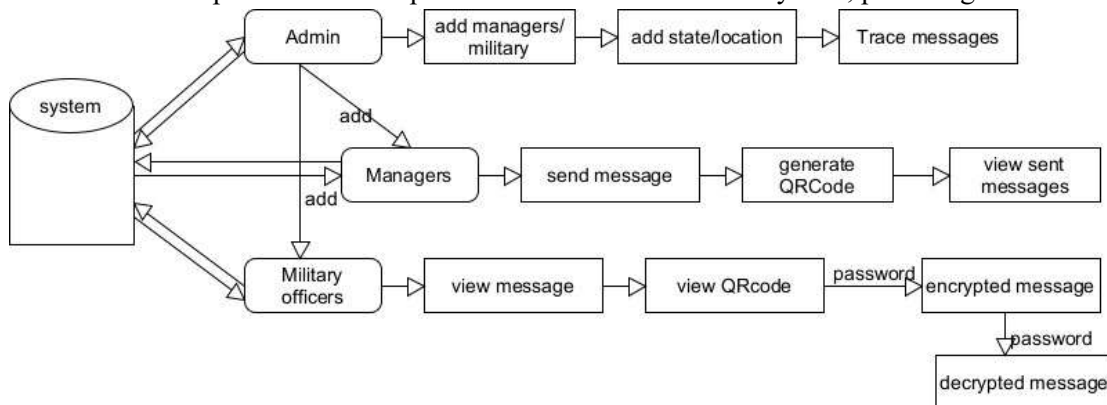
- **Usability:** The application we are developing will be utilized by managers or military officers, assisting them in sending messages to military personnel.
- **Efficiency:** Our application is designed to complete specific tasks, such as message sending, in a shorter time frame, thereby reducing time complexity. It simplifies processes when information encompasses multiple functionalities, thus enhancing overall efficiency.
- **Reliability:** The application we are creating is intended to securely deliver a set of messages. It includes various modules, each developed to meet the non-functional requirements of managers and military officers.
- **Maintainability:** The application we are developing aims to achieve high performance metrics, such as automatic data updates without compromising existing data.

3. SYSTEM DESIGN

A systemic approach is essential for ensuring a coherent and efficiently functioning system. Either a Bottom-Up or Top-Down approach is necessary to consider all relevant variables of the system. A designer employs modeling languages to articulate the information and knowledge within a system structure that is governed by a consistent set of rules and definitions. The designs may be represented using either graphical or textual modeling languages. Systems design involves defining the architecture, product design, modules, interfaces, and data necessary for a system to meet specified requirements. It can be viewed as the application of systems theory to the development of products.

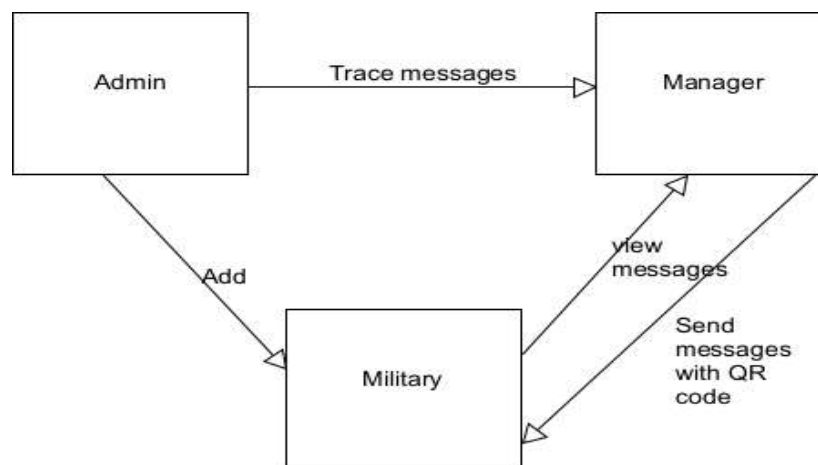
3.1 SYSTEM PERSPECTIVE

An architectural diagram serves as a representation of a system, utilized to abstract the overall outline of the software system along with the relationships, constraints, and boundaries among its components. The system architecture illustrated below presents the comprehensive architecture of the system, providing an overview of the entire system.

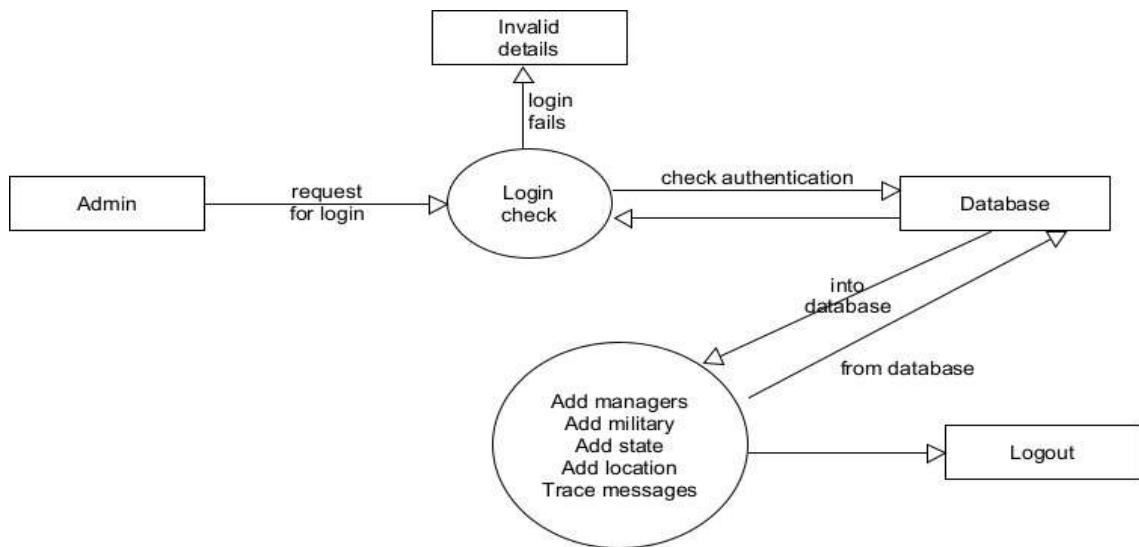


3.2 CONTEXT DIAGRAM

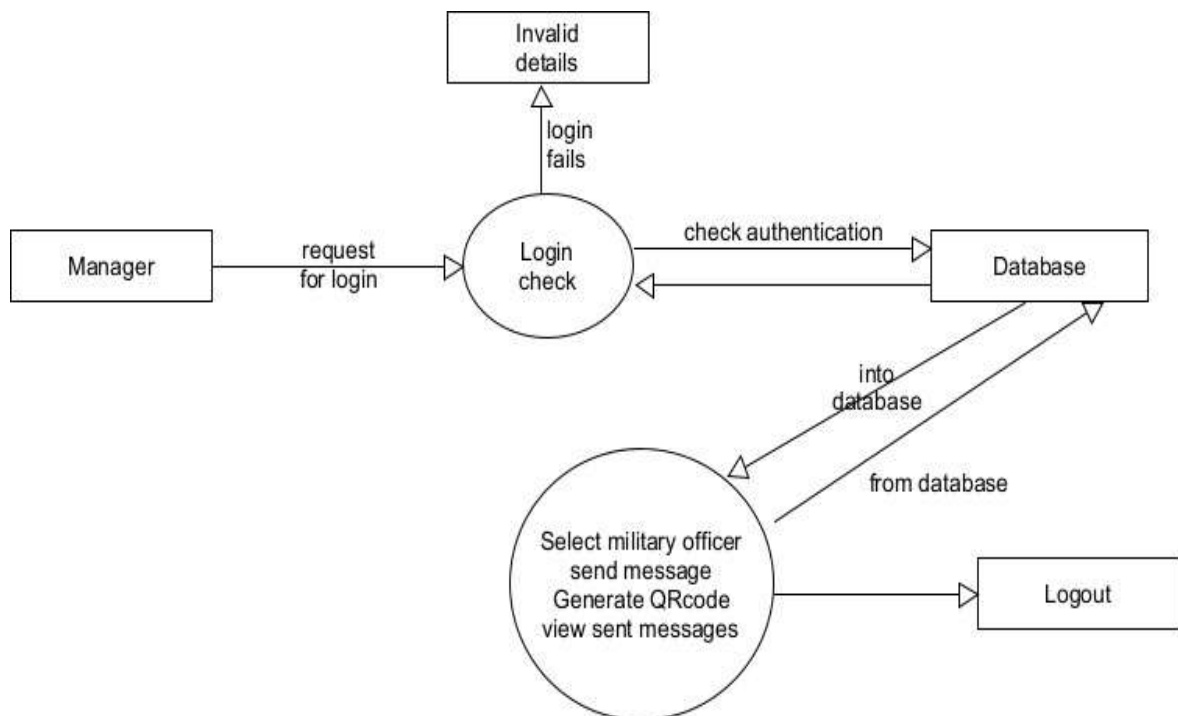
A context diagram, often referred to as a level 0 data-flow diagram, is created to delineate and elucidate the boundaries of the software system. It highlights the information flows between the system and external entities. The complete software system is represented as a singular process.



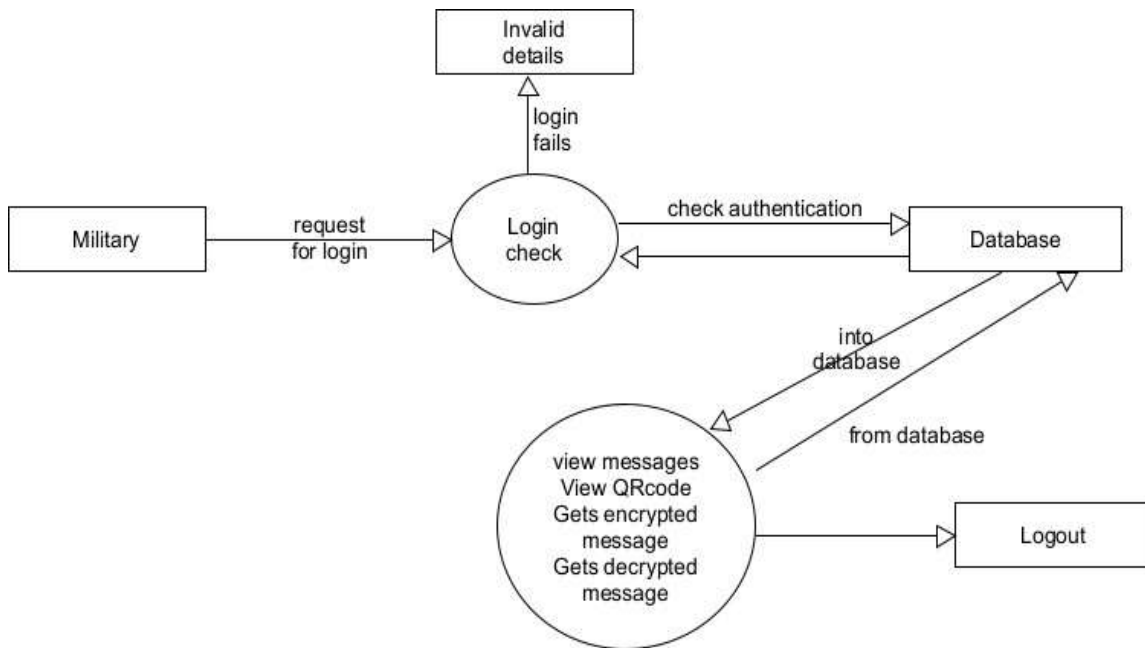
Admin



Manager



Military



4. TEST CASES

	Test case name	Test case description	Test steps				Test status
			Step	I/p given	Expected o/p	Actual o/p	
TC01	Login	To verify Admin/Manager and military login details	user login	Username & Password	Login Successfully	Login Successfully	pass
	Login	To verify Admin/Manager and military login details	Non Registered login	Username & Password	Login Successfully	Error Non Registered not allowed	Fail
TC02	Add	Admin manager/military state details	Admin Adds details	Admin adds details	Details are added	successful	pass
	Add	To add RTO/Police details	Admin Adds details	Admin adds details	Details are not added	Not successful	Fail

TC0 3	Trace Message	Admin trace message sent by individuals	Trace Message	Individuals Message	Individuals Message	successful	pass
	Trace Message	Admin trace message sent by individuals	Trace Message	Individuals Message	Individuals Message	Not successful	Fail
TC0 4	Send Message	Manger send messages to military officer	QR code is generate	Message	Message	successful	pass
	Send Message	Manger send messages to military officer	QR code is generate	Message	Message	Not - successful	fail
TC0 5	View message	Military view the encrypted message	Enter Password	Decrypted message	Decrypted message	Successful	pass
	View message	Military view the encrypted message	Enter Password	Decrypted message	Decrypted message	Not successful	Fail

5. CONCLUSION

In this paper, we introduce a steganography system that utilizes QR codes as containers for embedding messages. Rather than embedding messages within an image, we embed them directly into a QR code. This type of system is employed to securely transmit messages to military personnel. Furthermore, the message remains independent, allowing it to potentially mislead adversaries. The generated QR codes have been tested, and the results indicate that they are indistinguishable from standard QR codes. The recipient of the QR code decrypts the encrypted message using a password. Additionally, these codes are space-efficient and offer enhanced security compared to traditional image-based steganographic systems.

6. FUTURE ENHANCEMENT

Given the extensive range of options and the masking capabilities provided by widespread Internet usage, malware developers may discover significant potential in network steganography. Consequently, future work will involve conducting a more in-depth analysis to comprehend the steganography processes employed by both the hider and the masker. The research can be broadened by analyzing the steganography processes of various tools within audio and video media files. It is essential to model the maximum capacity of information that can be concealed within an image using a specific steganography tool.

BIBLIOGRAPHY

- [1] T. Morkel, J. H. Eloff, and M. S. Olivier, “An overview of image steganography,” in *Proc. ISSA*, 2005, pp. 1–11.
- [2] B. Dunbar, “A detailed look at steganographic techniques and their use in an open- systems environment,” in *The Information Security Reading Room*. Bethesda, MD, USA: SANS Institute, 2002.
- [3] S. R. M. Mary and E. K. Rosemary, “Data security through Qr code encryption and steganography,” *Adv. Comput., Int. J.*, vol. 7, nos. 1–2, pp. 1–7, Mar. 2016.
- [4] J. Waleed, H. D. Jun, S. Saadon, S. Hameed, and H. Hatem, “An immune secret QR- code sharing based on a twofold zero-watermarking scheme,” *Int. J. Multimedia Ubiquitous Eng.*, vol. 10, no. 4, pp. 399–412, Apr. 2015.
- [5] T. J. Soon, “QR code,” *Synth. J.*, vol. 2008, no. 3, pp. 59–78, 2008.
- [6] *Information Technology—Automatic Identification and Data Capture Techniques—QR Code bar Code Symbol Specification*, ISO/IEC Standard 18004:2015, 2015.
- [7] M. Charikar and D. Ramakrishna, “Lossless compression of fragmented image data,” U.S. Patent 16 276 411, Jun. 13 2019.
- [8] A. K. Sahu and G. Swain, “An optimal information hiding approach based on pixel value differencing and modulus function,” *Wireless Pers. Commun.*, vol. 108, no. 1, pp. 159–174, Sep. 2019, doi: [10.1007/s11277-019-06393-z](https://doi.org/10.1007/s11277-019-06393-z).
- [9] S. A. Kumar and S. Gandharba, “High fidelity based reversible data hiding using modified LSB matching and pixel difference,” *J. King Saud Univ.-Comput. Inf. Sci.*, to be published. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1319157819304124>, doi: [10.1016/j.jksuci.2019.07.004](https://doi.org/10.1016/j.jksuci.2019.07.004).