Reversible image stegnography Scheme Based on A U Net structure

Keerthana.C[1], Nandhini.S[2], Priyadharshini.K[3], Preeethi.G[4]
[1, 2, 3, 4] Dept of Computer science and Engineering,
[1, 2, 3, 4] TJS Engineering college

Abstract- *Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography called hidden text is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed in some way to increase the difficulty of detecting the secret content. Steganography is practiced by those wishing to convey a secret message or code. In this application, the user can hide and send the information in the form of Image, Barcode, etc. The data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as a JPEG image, audio or video file. The secret message can be embedded in ordinary data files in many different ways. The user can send the hidden data format and the secret key value to others from the application itself. The receiver must use the same application to decrypt the hidden data from the shared resource using the secret key. If they use some other application the user cant able to decrypt the data.*

I. INTRODUCTION

GENERALINTRODUCTION:

The growing use of Internet needs to take attention while we send and receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption. However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form. A solution to this problem has already been achieved by using a “steganography” technique to hide data in a cover media so that other cannot notice it. The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness. In this document, I propose a new system for hiding data stands on many methods and algorithms for image hiding where I store on data file, called sink file in an image file called as container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously using less storage.

DOMAININTRODUCTION :

- JAVA was developed by James Gosling at Sun Microsystems Inc in the year 1991, later acquired by Oracle Corporation. It is a simple programming language. Java makes writing, compiling, and debugging programming easy. It helps to create reusable code and modular programs
- Java is a class-based, object-oriented programming language and is designed to have as few implementation dependencies as possible.
- A general-purpose programming language made for developers to *write once run anywhere* that is compiled Java code can run on all platforms that support Java.
- Java applications are compiled to byte code that can run on any Java Virtual Machine. The syntax of Java is similar to c/ c++

JAVAFEATURES:

1. **Platform Independent**: Compiler converts source code to bytecode and then the JVM executes the bytecode generated by the compiler. This bytecode can run on any platform be it Windows, Linux, macOS which means if we compile a program on Windows, then we can run it on Linux and vice versa. Each operating system has a different JVM, but the output produced by all the OS is the same after the execution of bytecode. That is why we call java a platform-independent language.

2. **Object-Oriented Programming Language:** Organizing the program in the terms of collection of objects is a way of

object-oriented programming, each of which represents an instance of the class.

The four main concepts of Object-Oriented programming are:

- Abstraction
- Encapsulation
- Inheritance
- Polymorphism

3. **Simple:** Java is one of the simple languages as it does not have complex features like pointers, operator overloading, multiple inheritances, Explicit memory allocation.

4. **Robust:** Java language is robust that means reliable. It is developed in such a way that it puts a lot of effort into checking errors as early as possible, that is why the java compiler is able to detect even those errors that are not easy to detect by another programming language. The main features of java that make it robust are garbage collection, Exception Handling, and memory allocation.]

5**. Secure:** In java, we don't have pointers, and so we cannot access out-of-bound arrays i.e it shows Array Index Out Of Bounds Exception if we try to do so. That's why several security flaws like stack corruption or buffer overflow is impossible to exploit in Java.

6. **Distributed:** We can create distributed applications using the java programming language. Remote Method Invocation and Enterprise Java Beans are used for creating distributed applications in java. The java programs can be easily distributed on one or more systems that are connected to each other through an internet connection.

7. **Multithreading:** Java supports multithreading. It is a Java feature that allows concurrent execution of two or more parts of a program for maximum utilization of CPU.

8**. Portable:** As we know, java code written on one machine can be run on another machine. The platform-independent feature of java in which its platform-independent bytecode can be taken to any platform for execution makes java portable.

SCOPEOF THEPROJECT

This software project is intended to provide the transfer of secret message m embedded in the image data d, to obtain new data d', practically indistinguishable from the data d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'.

II. LITERATURE SURVEY

[1].J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities," in Proc. 9th ACM Workshop Multimedia Security, Dallas, TX, USA, Sep. 2007, The goal of this paper is to determine the steganographic capacity of JPEG images (the largest payload that can be undetectably embedded) with respect to current best steganalytic methods. Additionally, by testing selected steganographic algorithms . we evaluate the influence of specific design elements and principles, such as the choice of the JPEG compressor, matrix embedding, adaptive content-dependent selection channels, and minimal distortion steganography using side information at the sender.

[2].T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion insteganography using syndrome-trellis codes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 920–935, Sep. 2011. This paper proposes a complete practical methodology for minimizing additive distortion in steganography with general (no binary) embedding operation. Let every possible value of every stego element be assigned a scalar expressing the distortion of an embedding change done by replacing the cover element by this value. Without any loss of performance, the no binary case is decomposed into several binary cases by replacing individual bits in cover elements. The binary case is approached using a novel syndrome-coding scheme based on dual convolution codes equipped with the Viterbi algorithm. 2

[3].J. Kodovský and J. Fridrich, "Calibration revisited," in Proc. 11th ACM Workshop Multimedia Security, New York, NY, USA, Sep. 2009, pp. 63–74. The concept of embedding in steganography that minimizes a distortion function is connected to many basic principles used for constructing embedding schemes for complex cover sources today, including the principle of minimal embedding- impact , approximate modelpreservation, or the Gibbs construction. The current work describes a complete practical framework for constructing steganographic schemes and reproducing algorithm that embed by minimizing an additive distortion function. Once the steganographer specifies the form of the distortion function, the proposed framework provides all essential tools for constructing practical embedding schemes working close to their theoretical bounds

[4].Federal Information Processing Standards, Advanced Encryption Standard (AES). Federal Information Processing Standards Publications (FIPS PUBS), Nov 2001. High throughput AES encryption/decryption is a necessity for many of modern embedded systems. This article

presents a high performance yet cost efficient AES system. Maestro can be used in a wide range of embedded applicationswith various requirements and limitations. Maestro is about one million times faster than the pure software implementation. TheMaestro architecture is composed of two major components; the soft processor aimed at system initialization and control. The hardware AES engine for high performance AES encryption/decryption. A ten stage implicit pipelined 3

[5].S. Doyle, "Using short message service as a marketing tool", Journal of Database Marketing, vol. 8, no 3, 2001, pp. 273-277. Short Message Service (SMS) is a very popular way for mobile phone and portable device users to send and receive simple text messages. Unfortunately, SMS is does not offer a secure environment for confidential data during transmission. This paper deals with an SMS encryption for mobile communication on Android message application. The transmission of an SMS in mobile communication is not secure, therefore it is desirable to secure SMS by additional encryption. In this paper, there is proposed the use of 3D-AES block cipher symmetric cryptography algorithm for SMS transfer securing.

[6].MehrdadBiglari, EhsanQasemi, BehnazPourmohseni" Maestro: A High Performance AES Encryption/Decryption System"Nov. 2009. High throughput AES
encryption/decryption is a necessity for many of modern embedded systems. This article presents a high performance yet cost efficient AES system. Maestro can be used in a wide range of embedded applications with various requirements and limitations. Maestro is about one million times faster than the pure software implementation. The Maestro architecture is composed of two major components; the soft processor aimed at system initialization and control, and the hardware AES engine for high performance AES encryption/decryption. A ten stage implicit pipelined architecture is considered for the AES engine. 4

[7].Arvind Arasu1, Spyros Blanas" Orthogonal Security WithCipherbase" In CRYPTO, 2011. This paper describes the design of the Cipherbase system. Cipherbase is a full-fledged SQL database system that achieves high performance and high data confidentiality by storing and processing strongly encrypted data. The Cipherbase system incorporates customized trusted hardware, extending Microsoft's SQL Server for efficient execution of queries using both secure hardware and commodity servers. This paper presents the design of the Cipherbase secure hardware and its implementation using FPGAs. Furthermore, this paper shows how we addressed hardware / software co-design in the Cipherbase system

[8].E.Arikan,—Channel polarization:A method for constructing capacityachieving codes for symmetric binary-input memorylessm channels, IEEE Trans. Inf. Theory, vol. 55, pp. 3051–3073, Jul. 2009. ‖ AFASCINATING aspect of Shannon's proof of the noisy channel coding theorem is the random-coding method that he used to show the existence of capacity-achieving code sequences without exhibiting any specific such sequence . Explicit construction of provably capacity-achieving code sequences with low encoding and decoding complexities has since then been an elusive goal. So far we have considered only combining copies of one DMC . Another direction for generalization of the method is to combine copies of two or more distinct DMCs..

[9]. Arvindarasu, ken eguro" a secure coprocessor for database applications"vldb 2011 vol. 4, 1359-62. In this paper, we describe a novel secure FPGA-based query coprocessor and discuss how it can be tightly integrated with a commercial database system such as SQL Server. This combination, called Cipher base, leverages efficient division of labor using a conventional entrusted cloud server to handle mundane database operations while sensitive data is segregated and processed in trusted hardware to ensure confidentiality. We examine the architectural design issues that affect the achievable performance of the system and report initial results demonstrating the effectiveness for real-world cloud database applications.

[10]. SuriyaniAriffin,Faculty" SMS Encryption using 3D-AES Block Cipher on Android Message Application" vol. 8, no 3, 2013. Short Message Service (SMS) is a very popular way for mobile phone and portable device users to send and receive simple text messages. Unfortunately, SMS is does not offer a secure environment for confidential data during transmission. This paper deals with an SMS encryption for mobile communication on Android message application. The transmission of an SMS in mobile communication is not secure, therefore it is desirable to secure SMS by additional encryption. In this paper, there is proposed the use of 3D-AES block cipher symmetric cryptography algorithm for SMS transfer securing. The experiment, the 3D-AES has low encryption time when message size is more then 256 bits.

III. EXISTING AND PROPOSED SYSTEM

Existing System:

Previously we have used a system which only hides the information in the master file and it supports only few formats of master files.

¬ This system doesn't support the encryption and also compression. Here we can hide only the message and it won't supports hiding of files.

¬ Existing systems affects the little bit originality of master file and the overall process is little bit complex, consumes much time.

Drawbacks:

¬ Significant damage to picture appearance. Message difficult to recover.

¬ Relatively easy to detect, as our project has shown.

¬ Image is distorted. Message easily lost if picture subject to compression such as JPEG.

¬ Message is hard to recover if image is subject to attack such as translation and rotation

THE PROPOSED SYSTEM:

¬ we are going to embedded both the message and file in the master file. It also supports large amount of information to be embedded.

¬ Our system supports many formats of the master files like image, audio and video files and also our system supports both the encryption and compression.

¬ Crypt analysis is difficult in our system because of the powerful algorithm and length of the password. 3.2.1

ADVANTAGES OF PROPOSED SYSTEM:

¬Hard to detect Original image is very similar to altered image. Embedded data resembles Gaussian noise.

¬ Hard to detect as message and fundamental image data share same range.

¬ Altered picture closely resembles original. Not susceptible to attacks such as rotation and translation.

SOFTWAREREQUIREMENTS:

The purpose of the Software Requirement Specification is to produce the specification of the analysis task and also to establish complete information about the requirements, behavior and other constraints such as functional performance and so on

HARDWARE REQUIREMENTS:

Processor : Intel i5
RAM : Min 4 GB
Hard Disk : 400 GB

Operating system: Windows 10
Technology Used: Android 9
IDE: Eclipse
Plug-in: ADT plug-in
Tools used: Android

IV. CONCLUSION

The application has been successfully developed, fulfilling the necessary requirements, as identifies in the background study and requirements analysis phase. The design of the system IS flexible and has a consistent flow for easy understanding. This is to ensure that enhancements can easily accommodate, without having to make major changes to the application. The software is developed with scalability in mind. Additional modules can be easily added when necessary. The software is developed with a modular approach. All modules in this project have been tested separately and put together to form the main system. Finally, the system is tested with real data and everything worked successfully. Some of the difficulties that did arise during the execution were solved with the help of our department staff member. It may also be concluded that with the technical background that we are having how is sufficient to complete any software project . Finally, to conclude, the software development was completed and accepted by the management as well as the user, staff.

V. ACKNOWLEDGEMENT

"Project is the product out of experience that goes a long way in shaping up a person's caliber. The experience and success on eat tains is not by one self but with a group of kind hearts behind."

First and foremost, we express our sincere thanks to honorable Founder and Chairman "**KALVINERIKAVALAR**" **Shri.T.J.GOVINDARAJAN** B.A., Managing Director & Secretary Shri. **T.J.ARUMUGAM**., Vice Chairman **Shri.**

T.J.DESAMUTHU., Directors **Dr.A.PALANIB.D.S**., **Shri. A.VIJAYA KUMAR B.E Ph.D**., **Shri. A.KABILAN** BA.B.L..M.B.A.,**Shri.D.DINESH**B.Com.,L.L.B.,**Shri.G.TA MILARASAN** B.Com..,M.B.A., for providing us with adequate infrastructure and congenital academic environment. We also record our sincere thanks to our honorable Principal **Dr. A.VIJAYAKUMAR Ph.D.,** for his kind support to take up this project.

We express our gratitude to **Mr.AVB DAKCHINAMOORTHY M.E(CSE).,** $\overline{Ph.D}$**.,** Head of the Department of Computer Science and Engineering whose guidance and encouragement has helped using completing this project work.

We extend our sincere thanks to our guide **Mrs. S.V PRIYANKA M.E (CSE)** and all other **TEACHING FACULTIES** and **NON-TEACHINGSTAFF** of Department of Computer Science and Engineering for giving the confidence to complete the project successfully by providing the valuable suggestions and interstate very stage of the project.

Further the acknowledgement would be incomplete if we would not mention a word thanks to our most beloved **PARENTS** and **FRIENDS** whose continuous support and encouragement all the way through the course has led us to pursue the degree and confidently complete the project.

REFERENCES

[1] Duan, X., Jia, K., Li, B., Guo, D., Zhang, E., & Qin, C. (2019). Reversible image steganography scheme based on a U-Net structure. IEEE Access, 7, 9314-9323.

[2] Duan, X., Liu, N., Gou, M., Wang, W., & Qin, C. (2020). SteganoCNN: Image Steganography with Generalization Ability Based on Convolutional Neural Network. Entropy, 22(10), 1140.

[3] Li, C., Jiang, Y., &Cheslyar, M. (2018). Embedding image through generated intermediate medium using deep convolutional generative adversarial network. Computers, Materials & Continua, 56(2), 313-324.

[4] Liu, H. H., & Lee, C. M. (2019). High-capacity reversible image steganography based on pixel value ordering. EURASIP Journal on Image and Video Processing, 2019(1), 54.

[5] Huang, L. C., Tseng, L. Y., & Hwang, M. S. (2013). A reversible data hiding method by histogram shifting in high quality medical images. Journal of Systems and Software, 86(3), 716-727.

[6] Lin, P. Y., & Chan, C. S. (2010). Invertible secret image sharing with steganography. Pattern Recognition Letters, 31(13), 1887-1893.

[7] Duan, X., Guo, D., & Qin, C. (2020). Image Information Hiding Method Based on Image Compression and Deep Neural Network. Computer Modeling in Engineering & Sciences, 124(2), 721-745.

[8] Wang, W. J., Huang, C. T., & Wang, S. J. (2011). VQ applications in steganographic data hiding upon multimedia images. IEEE Systems Journal, 5(4), 528-537.

[9] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network. IEEE Access, 8, 25777-25788.

[10] Muhammad, K., Ahmad, J., Sajjad, M., & Zubair, M. (2015). Secure image steganography using cryptography and image transposition. arXiv preprint arXiv:1510.04413.