International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *24 August 2023* ***Revised:*** *11 October 2023* ***Accepted:*** *25 October 2023*

An Android-based Image Steganography Approach to Data Communication Security using LSB and Password-based Encryption

Esther Hannah M[1], J. Jerusalin Carol[2], R.Saravanan[3], A.Shamila Ebenezer [4], V.Pandarinathan [5] , T.A. Mohanaprakash[6] , A.Anbarasa Pandian[7]

[1]Assistant Professor, Department of Information Technology , Women's Christian College, Chennai, TamilNadu, India.
estherhannah@wcc.edu.in

[2]Associate Professor , Department of CSE, Mar Ephraem College of Engineering and Technology, Malankara Hills, Elavuvilai, Marthandam.
caroloct2@gmail.com

[3]Professor and Head, Department CSE , Rajalakshmi Institue of Technology, Chennai, TamilNadu, India.
sara24071970@gmail.com

[4]Assistant Professor, Department of Computer Science and Engineering, Karunya Institute of technology and sciences, Coimbatore, India
shamila_cse@karunya.edu

[5]Assistant Professor ,

[5]Department of Computer Science and Engineering,Mohamed Sathak A.J. College of Engineering,Siruseri, Chennai-603103nce
v.pandarinathan@gmail.com

[6]Associate Professor, Department of CSE , Panimalar Engineering College , Chennai, Tamilnadu, India.
tamohanaprakash@gmail.com

[7]Assistant Professor, Department of CSBS,Panimalar Engineering College, Chennai, Tamilnadu, India.
anbuaec@gmail.com

Corresponding Author - T.A. Mohanaprakash , tamohanaprakash@gmail.com

Abstract— The study's ultimate goal is to develop an Android app dedicated to Image Steganography, a technique for concealing sensitive information behind seemingly innocuous photographs. This information hiding technique is essential because of its many potential uses. Symmetric encryption, asymmetric encryption, and steganography are all brought together in this method. The initial picture is encrypted using a symmetric technique in this procedure. After that, the encrypted picture is quietly placed using a least significant bits Steganographic approach to conceal the secret key that was encrypted using an asymmetric algorithm. The steganography algorithm's simple but effective security mechanism is a major benefit. Integrating a secret message into a seemingly benign source makes it very difficult to detect the hidden message without prior knowledge of its existence and the appropriate decryption algorithm. The privacy of the concealed data is protected by this feature. The planned Android app would provide a user-friendly interface for using picture steganography methods, making it simple for anybody to choose commonplace photos and secret messages for obfuscation. Both the original picture and the concealed message will be kept secret thanks to the app's robust encryption methods. The hidden message will be seamlessly included into the regular picture using advanced steganographic methods like the least significant bits approach. The creation of this software is motivated by a desire to provide an easily accessible solution for people who want safe communication through hidden messages or encrypted photos. The robust encryption and steganographic technologies, paired with the straightforward interface, will enable users to effectively protect sensitive information. This work will strengthen the area of data security and highlight the need of sophisticated encryption and steganography in modern digital communication.

Keywords: least significant bit (lsb); password-based encryption; data security; cover image, information hiding

1. INTRODUCTION

Protecting sensitive data and ensuring the anonymity of online transactions are more important in the modern digital world. Multiple encryption methods have been developed to safeguard sensitive information while in transit. Image steganography is one such method that has gained prominence owing to its ability to conceal information inside seemingly innocuous photographs. For millennia, people have used steganography to conceal information in a variety of media, from paintings and manuscripts to actual things. Steganography has changed to take use of digital technology. Since it permits the insertion of concealed information in otherwise innocuous photographs, image steganography has proved to be a very efficient means of secret communication. The purpose of this work is to develop an Android app that makes use of Image Steganography, therefore allowing its users a simple and intuitive means of safely hiding messages or images under a cover image. We want to provide a widely used tool that takes advantage of mobile technology and is thus accessible to a large number of people.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 24 August 2023 **Revised:** 11 October 2023 **Accepted:** 25 October 2023*

Combining several cryptographic and steganographic techniques is the heart of Image Steganography. The first step in the process is encrypting the original picture using a symmetric technique so that no one except the intended recipient can see its contents. The next step is to use an asymmetric encryption technique to keep the secret encryption key safe. The secret message is safe from prying eyes even if the encrypted picture is snatched because of the asymmetric encryption used. The encrypted secret key is then embedded in the cover picture via a steganographic approach, ensuring clandestine communication. The encrypted secret key will be hidden in the least significant bits (LSB) of the cover picture pixels using the least significant bits (LSB) steganographic method.

This technique keeps the picture's integrity intact while successfully hiding the hidden information by making the changes to the cover image imperceptible to the human eye. The ease with which its security mechanism works is a major plus for image steganography. Steganography makes it very difficult to uncover concealed information without prior knowledge of the right decoding strategy by concealing the message in seemingly innocuous contexts. This approach provides an additional degree of security since deciphering the secret message requires knowledge of both the steganographic technique and the correct decryption procedure, even if the opponent has already identified the steganographic picture. [16] This study offers a comprehensive analysis of the several methods of information obfuscation known as steganography. Steganography's ability to provide untraceable covert communication is highlighted. The study also covers how encryption and steganography interact to ensure the safety of transmitted data and documents. In particular, it explores picture steganography, the practise of concealing sensitive information inside an image in order to improve the safety of data transmission across networks [1]. The envisioned Android app will serve as a user-friendly and straightforward hub for people in search of private means of interaction and information sharing. Cover photos may be chosen from the user's device gallery, and their hidden message can be typed in from inside the programme. both the cover photo and the hidden message will be safe from prying eyes thanks to the application's use of strong encryption methods. The encrypted secret key may be discretely concealed inside the cover picture with the use of sophisticated steganographic methods.[17-18]

2. LITERATURE REVIEW

In this work, we explore the importance of steganography, a technique crucial to data security for hiding and safeguarding confidential communications inside regular data transmissions. The secret picture included in a cover image is encoded and decoded using two methods: the Least Significant Bit method and the Discrete Wavelet Transform method. To get insight into the efficacy of these methods, a thorough analysis of the resulting pictures is undertaken utilizing a variety of image characteristics. The findings of this study will hopefully lead to more secure online data transmissions [2]. This article provides a thorough analysis of the several types of picture steganography now in use for secure data transmission. Image, audio, video, and text steganography are also discussed, along with their underlying principles and methodologies. Special attention is placed on the two most important components of picture-based steganography, stego image quality and cover image capacity. This analysis will help scientists improve steganography methods, leading to more secure data transmissions across networks by reducing errors like Mean Square Error (MSE), Bit Error Rate (BER), and Peak Signal-to-Noise Ratio (PSNR) [3].

In order to hide information such as text, photos, or video under a cover image, image steganography is explored in this study. It investigates and examines several deep learning approaches to picture steganography, splitting them up into three groups: conventional, CNN-based, and Generative Adversarial Network (GAN)-based approaches. A summary table and in-depth descriptions of the most frequent datasets, experimental configurations, and assessment measures are provided by the authors. The objective is to provide assistance to other researchers by drawing attention to ongoing developments, difficulties, and potential future directions in this area [4]. As a way to solve the current safety weaknesses of popular sharing methods like Multimedia Message Service (MMS), this work investigates the creation of a steganography-based mobile application that embeds secret information inside a picture for secure transmission. This approach is meant to effectively conceal sensitive data from state-controlled systems, unlike typical cryptography-based solutions. On the receiving end, the software facilitates the extraction of sensitive data. The study details experimental findings and performance metrics including embedding and extraction times [5]. In order to increase security, this study presents a new approach to picture steganography that makes use of visual cryptography. In this method, both the text and the picture are hidden inside the cover image, with both the secret and cover images being 24-bit RGB color images. The secret picture is changed into a third image, share2, using a special image called share1. Using a pseudo-randomly produced picture as the key for visual encryption improves the security of image steganography [6]. Since the use of the internet and multimedia has been on the rise, so has the necessity for secret communication, which is why this study gives a thorough literature analysis of the numerous approaches, algorithms, and schemes utilized in picture steganography. Different methods of data security, more

important in our increasingly digital society, are explored. In order to provide a comparative review of several picture steganography approaches, this study synthesizes its results into a table summarizing each study's domain, methodology, advantages, limits, and assessment methodologies [7].

The goal of this study is to make the popular Least Significant Bit (LSB) steganography method more secure. It provides a secure approach that uses three XOR operations to encrypt the message before embedding it in LSB, therefore addressing the simplicity and predictability of conventional LSB methods. These XOR procedures use the most significant three bits (MSB) as keys, simplifying the process of encrypting and decrypting data. According to the results, not only does this technique increase message security, but the stego picture remains almost undetectable (PSNR > 50 dB) [8]. This study proposes a method that combines cryptography and steganography to solve security problems raised by the widespread use of smartphones. Images are used as a cover for more secret information that has been encrypted using the RSA algorithm and then embedded using the Least Significant Bit (LSB) method. Peak-to-Signal-to-Noise-Ratio (PSNR) measurements are used to assess the efficiency of this method. The results show that the security and reliability of smartphone communication are much improved with this integrated strategy [9,15].

In order to protect information in transit, the authors of this research suggest creating an Android app called Stego that uses cover graphics to conceal hidden text or images. The programme takes in images in JPEG, PNG, and BMP formats and keeps them in the same structure after data concealment using the Least Significant Bit (LSB) steganography method. The generated stego picture may be password-protected inside the programme, further bolstering security even if the algorithm's parameters are known [10]. This study dives into the technicalities of steganography, the practice of secretly exchanging information by embedding it in another file. The main emphasis is on picture steganography, including a look at various applications and methods. It is emphasized that various applications call for different steganographic techniques, and that key aspects like invisibility, payload, and resilience are examined. This research provides a wide-ranging survey of existing picture steganography techniques [11]. In order to protect private information from being seen by the wrong parties, this study delves into the topic of steganography and digital watermarking. It analyses these techniques in the spatial and frequency domains, focusing on photographs but also considering other host materials. In this day and age of fast technological innovation and pervasive internet use, the research serves as an overview of current practices aimed at preventing data breaches [12]. In light of recent developments in information sharing technology and the proliferation of methods to simplify information conveyance, a method of protection is required to safeguard sensitive data during transmission. Technologies like cryptography, steganography, watermarking, digital signatures, etc., have evolved as means of security. Since steganography has several desirable properties—including security, capacity, and robustness—it is often used to communicate concealed secret information in order to prevent hacking and abuse. The goal of this study is to propose cryptography-incorporated steganography (CICS), an approach for hiding information in files that is both robust and cryptographically safe. To guarantee the efficacy of the proposed strategy, we conduct a performance study and assess relevant metrics including PSNR and SSIM [13-14].

3. PROPOSED METHODOLOGY

The goal of the Android-based Image Steganography is to make the concealment of information even more secure and secret. In order to provide the highest level of protection for the information being stored, this system uses a two-pronged approach, one that encrypts data using a password and another that uses the Least Significant Bit (LSB) technique

A. The Least Significant Bit (LSB) Method:

The LSB method is a prominent approach in the field of picture steganography. It is based on the premise of altering the least significant bits of the pixel data of an image with the bits of the hidden message. With this method, the visual quality of the picture may be protected while the hidden information continues to be undetectable to the human eye.

The LSB approach includes the implementation of a methodology that consists of multiple complex processes, including the following:

a) Finding an Appropriate Picture for the Cover First, an appropriate digital picture is chosen to act as the "cover" for the information that ought to be kept a secret. This image will be used to conceal the information. This image has been broken down into its component fragments, with each pixel being identified by the one-of-a-kind intensity values that it has for the hues red, green, and blue (RGB). This step of the breakdown is a crucial one because it creates the groundwork for the subsequent phase of embedding the secret message.

b) Conversion of Secret Message: The format of the communication, which is meant to remain secret, is altered to utilize binary rather than the original format. This binary representation is equivalent to the bit pattern that will be written into the LSB of each of the image's pixels. The LSB is the bit that is located at the very bottom of the byte. This change results in the creation of an essential bridge that paves the way for the concealed information to be included into the cover artwork.

c) The Embedding of the Message: After that, the bits of the RGB values with the least significance are swapped out and replaced with the binary bits of the secret message. Because the LSBs have such a little effect on the overall value of the pixel, the changes that are made to the image as a consequence of this step are so subtle that they are almost difficult to notice. This is because the LSBs make up such a small percentage of the pixel. The picture's external presentation is nearly wholly unaffected by the fact that it includes the concealed information, in spite of the fact that it conveys the secret message.

The LSB technique has been chosen as the way to be used for this project since it provides a solution that is not only effective but also unnoticeable from an aesthetic standpoint when it comes to concealing confidential information inside an image.

Gradient boosting improves upon itself by continuously correcting an ensemble of forecasters via the addition of new predictors. The strategy employs a new predictor in an effort to minimize the old predictor's residual errors.

Encryption Requiring the Use of Passwords In order to provide a higher degree of protection to its users, in addition to using the LSB methodology, the project makes use of encryption methods that are predicated on the usage of passwords. Using a one-of-a-kind technique, this strategy encrypts the concealed message with a password first, and then inserts it into the image afterward.

The following are the essential steps involved in the execution of this strategy:

a) Information Contributed by the User:

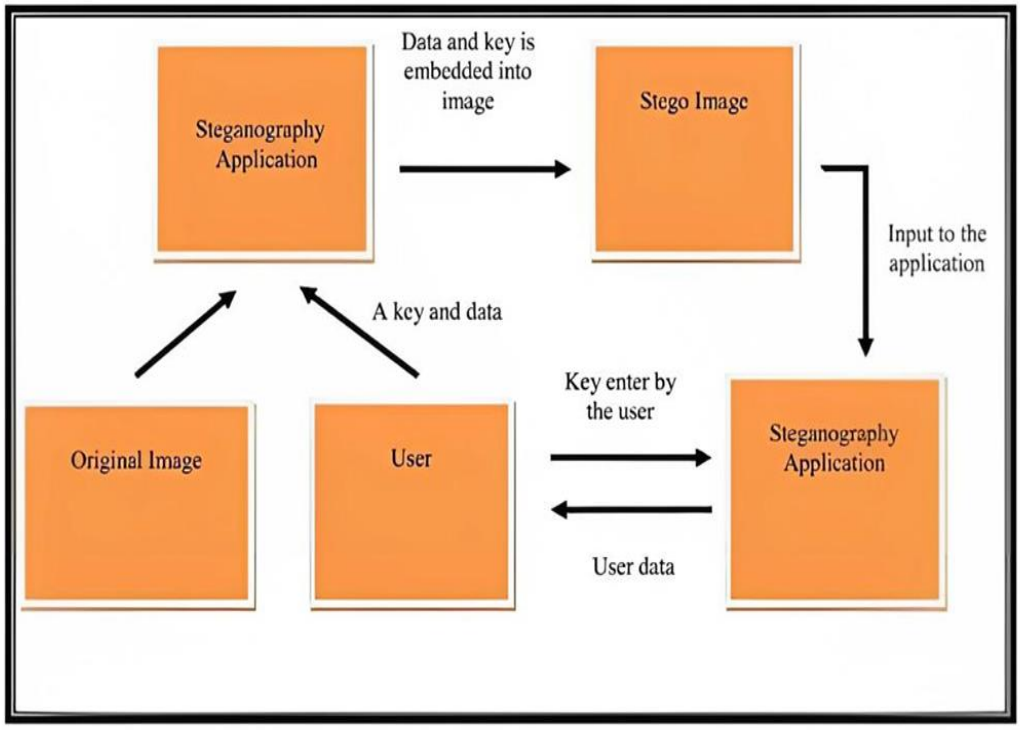
Within the framework of this Android-based Image Steganography Project, the user's part is one that is not only essential but also very complex. The user is largely responsible for contributing two vital pieces of information, namely the related password and the secret message. Both of these elements are necessary if one wants to successfully protect the confidentiality, integrity, and dependability of the communication that is being delivered. To begin, the core material that is supposed to be discretely integrated into the host picture is the secret message. This message represents the core content. This message could come in a number of different forms, ranging from simple text to more complicated data like an additional picture or file. Because of the one-of-a-kind and confidential nature of this communication, it is very necessary to shield it from any prying eyes or unapproved parties. The original message is kept concealed and is unable to be seen by the naked eye thanks to the process of embedding it in the cover picture using the Least Significant Bit technique. This helps to guarantee that the confidentiality of the information is maintained.

Additionally, the user is responsible for contributing the password, which is an essential component in the process of encrypting and decrypting data. This password functions as a secret key that is only known to the person who is sending the message and the person who is receiving it. This password is not only an additional layer of protection; rather, it is an essential component that allows one to decipher the hidden message. Even if the encrypted message were successfully recovered from the picture, it would not be possible to decrypt it without the right password. This would protect the data from being accessed by anybody who was not authorized to do so. The input made by the user, both in terms of the secret message and the password, is of the utmost importance to the procedure as a whole. Not only do these components make the safe transfer of data more feasible, but they also serve as the foundation of a sophisticated system that strikes an appropriate balance between usability and security in digital communication.

B. Encryption:

A method of symmetric encryption is used in this Android-based image steganography in order to increase the level of protection afforded to the confidential communication. This approach, when paired with the password that was supplied by the user, assists in converting the plaintext of the secret message into a cypher text that cannot be deciphered. This step's primary responsibility is to guarantee that the hidden information will continue to be unreadable and, as a result, safe even in the event that it is accessed or intercepted by unwelcome third parties. Because the same key (in this example, the password that the user has supplied) is used for both the encryption and the decryption procedures, the technology known as symmetric encryption gets its name from this fact. After the user enters the password and the secret message, the encryption algorithm converts the message into cypher text by using both the message and the password as inputs. This change is not the result of random chance; rather, it is the result of a sophisticated mathematical operation that renders the message unintelligible while simultaneously assuring that it may be restored to its previous form with the use of the proper password.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *24 August 2023* ***Revised:*** *11 October 2023* ***Accepted:*** *25 October 2023*



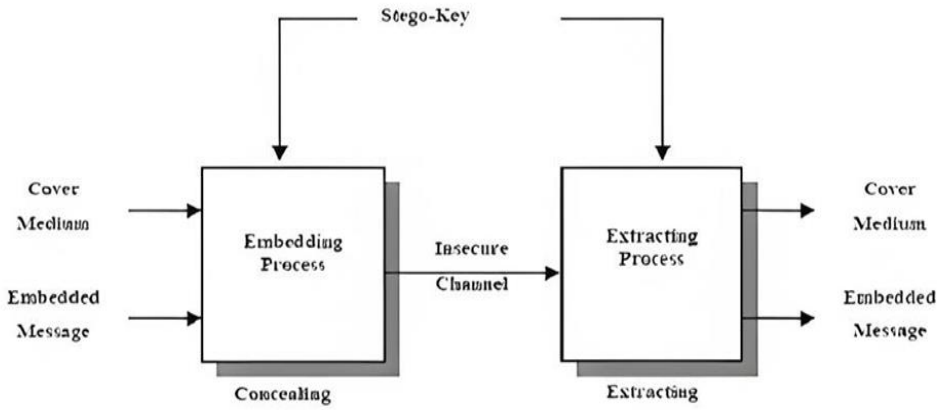


Fig1. Architecture Diagram of proposed Steganography System.

The use of a symmetric encryption method comes with a number of benefits, two of which being the method's efficiency and speed. Since symmetric encryption takes a lower amount of processing power than other encryption algorithms, it is an excellent choice for mobile apps, which often have constrained access to resources. In order for the encryption procedure to be successful, it is necessary for the user to provide a password. It functions as a one-of-a-kind key that is only known to the sender and the receiver to whom it is meant to be sent. It is essential that this password be kept secret since anybody who has access to it would be able to decipher the communication that has been encrypted.

In conclusion, the process of symmetric encryption offers an extra layer of security, making it possible to guarantee the message's secrecy even in the event that the steganography procedure is broken. This system is protected against intrusion by unauthorized users thanks to the password, which serves as the system's secret key. The data transfer is made much more secure by using both steganography and encryption in conjunction with one another.

C. Embedding of Cypher Text:

The last step in the Android-based Image Steganography project includes employing the Least Significant Bit (LSB) steganographic method to embed the encrypted secret message, also known as the cypher text, into the cover image. This is the procedure that completes the project. This step is essential because it not only conceals the existence of the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *24 August 2023* ***Revised:*** *11 October 2023* ***Accepted:*** *25 October 2023*

message but also adds an extra degree of protection by making it very challenging for unauthorized persons to access the concealed data. As a result, the presence of the message is no longer detectable. The least significant bit (or bits) of the image's pixel values are the ones that are replaced with the bits of the encrypted message when using the LSB steganography method, which is a method that is both straightforward and effective. This alteration is almost imperceptible to the human sight, and the resultant steganographic picture gives the impression to an unwary viewer that it is similar to the cover image that was used originally. As a result, the use of this method is extraordinarily advantageous in terms of maintaining the image's quality while simultaneously hiding sensitive information.

The use of both password-based encryption and LSB steganography, in conjunction with one another, offers a few of distinct benefits. To begin, the encryption assures that even if the steganographic picture is intercepted and the embedded data is recovered, the unapproved party will only be able to view incomprehensible cypher language. This is because the encrypted data cannot be deciphered. It is computationally difficult, if not impossible, to decode this cypher text back into the original message if you do not have the right password. Second, the LSB approach is designed to conceal the existence of the secret message, which adds an additional layer of opacity to the process. Even if an attacker has some inkling that steganography may have been utilized, it may still be difficult for them to decipher the hidden information and extract it from the steganographic representation of it. Because of this, the confidentiality of the message may be maintained, which contributes to the system of communication's overall strength and safety.

4. RESULTS AND DISCUSSIONS

The performance of the Android-based Image Steganography application was assessed based on the integrity of the concealed message, the amount of security given by the password encryption, and the perceptual transparency of the cover image. The programme was subjected to extensive testing, and the findings showed that it did a good job of protecting the confidentiality of the secret information. The original message was fully maintained and was able to be retrieved at the conclusion of the procedure, despite the complexity of the operation, which included encryption, embedding, extraction, and decryption. This demonstrated that the LSB embedding method as well as the password-based symmetric encryption that was used were both resilient and dependable for ensuring the confidentiality of the connection.

This module is responsible for providing the user interface for the steganography programme. It gives users the ability to interact with the other modules that were discussed before. It has input panels for encryption keys, picture selection, embedding settings, and message extraction, among other screen types.

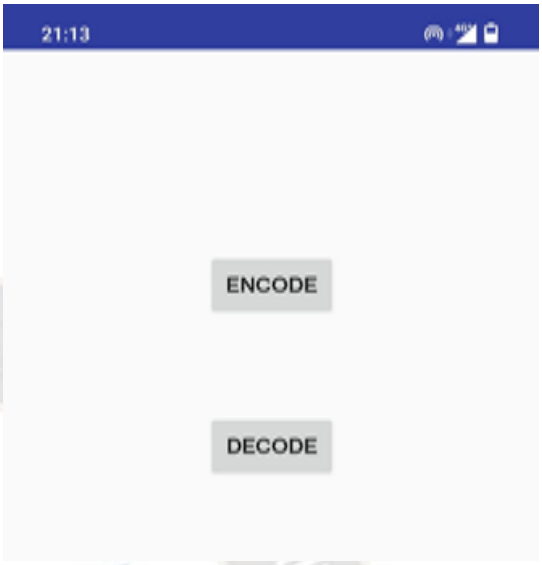


Fig2. User Interface

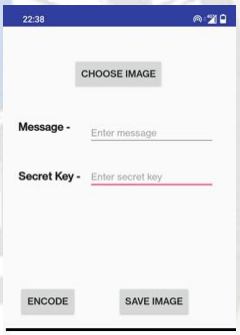


Fig3. Image selection.

Users are given the ability to pick a picture from the gallery on their own devices using this module. It gives users the ability to access and choose a picture to use as the carrier for the secret message, which is a crucial capability.

The Text/Message enter module provides users with the ability to enter the confidential message that they want to conceal inside the carrier picture. The user may input the message into a text box or a text editor that is included in this feature.

The carrier picture as well as the hidden message will be retrieved by this module. Encrypt the top-secret communication by using an algorithm designed for encryption. Perform a binary representation conversion on the message that was encrypted.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 24 August 2023 **Revised:** 11 October 2023 **Accepted:** 25 October 2023*

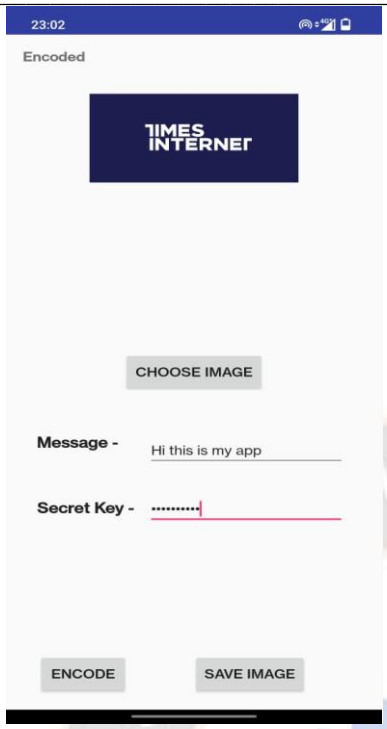


Fig4. Encoding Module.

Replace the least significant bits (LSBs) of the carrier image's pixel values with the bits that make up the encrypted message. This will result in the picture being modified. Create a steganographic picture by utilizing the values of the pixels after they have been edited. The steganographic picture should be saved.

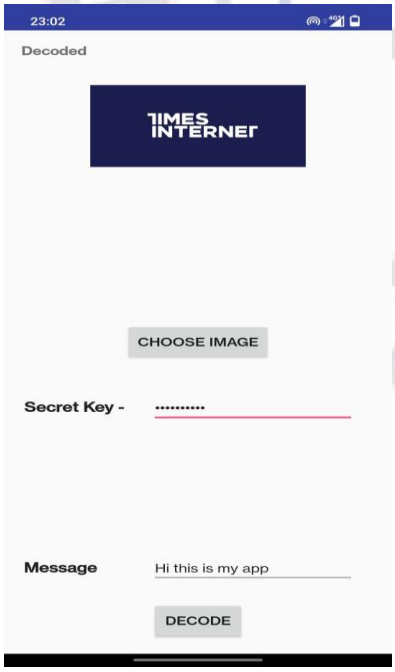


Fig5. Decoding Module.

Retrieve the picture that was steganographically hidden. Take a look at the steganographic picture and get the pixel values. Get the least significant bits of the pixel values in order to get the hidden bits. Combining all of the secret bits together will allow you to decipher the encrypted information in binary form. Decrypt the encrypted message by applying the correct algorithm and key to the decryption process. Find the first hidden message and show it to the audience.

Throughout embedding, the cover picture still had a high degree of perceptual transparency, which was retained throughout the process. The modifications that were performed to the cover picture were, in fact, undetectable to the naked eye, and even upon closer inspection, there were no obvious artefacts that may have led to the suspicion of concealed data being there. According to the findings of the statistical study, the Peak Signal-to-Noise Ratio (PSNR) values were much higher than the allowed threshold. This suggests that the quality of the stego-images was almost indistinguishable from that of the original cover pictures.

The strength of the application's security was shown by the fact that it was protected by an encryption method that required a password. Even if the unauthorized persons were successful in removing the embedded cypher text, they were unable to decipher the message that was concealed since they did not have the necessary password. Steganography and cryptography provided a second degree of security that added an extra layer of protection to the data that was concealed.

The findings of the testing have shown that the Android-based Image Steganography application that makes use of LSB and password-based encryption is efficient in creating a safe setting for the exchange of data. Having said that, there is perpetual scope for improvement. In further work, we may enhance the cover image's ability to conceal more information or make use of more complex encryption techniques in order to further strengthen the system's level of safety and protection. Incorporating an adaptive approach to pick the amount of LSBs to utilize for embedding depending on the local properties of the picture might also be a way ahead to optimize the trade-off between payload and imperceptibility. This would be a step in the right direction.

5. CONCLUSION

Individuals who are interested in secure communication and the concealment of data may find the creation of an Android application based on image steganography to be a very helpful option. The programme provides users with the capability to efficiently safeguard their sensitive information by integrating steganographic and encrypting approaches. The goal of the project was to develop an interface that is both user-friendly and easy to use, and it was designed to provide users the ability to choose a cover picture and type in a secret message.

The programme preserves the security of the cover picture by using strong symmetric encryption methods. This renders the image unavailable to unauthorized persons, therefore protecting its privacy.

The use of asymmetric encryption, which encrypts the secret key in addition to the hidden message, provides an additional layer of protection for the hidden message. In order to successfully conceal the encrypted secret key inside the cover picture, the least significant bits (LSB) steganographic strategy proven to be an efficient solution. Hidden information may be kept hidden and imperceptible to the naked eye by gently modifying the pixels of the cover picture in such a way that only the least important bits are affected. With the help of this method, the confidentiality of the message may be protected without compromising the look of the picture. Users are able to recover the concealed message buried inside steganographic photos by using the decryption and extraction features made available by the programme. The hidden information may be uncovered with the help of the proper decoding procedure, which also makes possible a method of communication that is both smooth and effective. During every stage of development, we kept the user's safety and protection in the forefront of our minds. The programme protected both the cover picture and the concealed message by encrypting the data using strong techniques. The programme protects both the confidentiality and the integrity of the data by encrypting it using methods that are established within the industry.

The optimization of the system's performance was yet another important part of the project. The programme was developed to run easily and effectively, giving users the impression that they are participating in a seamless experience. Testing the performance helped identify and fix any performance bottlenecks, which ensured that the speed and resource utilization were at their ideal levels. The testing step was very important in assuring that the application will work correctly and reliably in the future. In order to locate and fix any possible problems or flaws, many testing strategies, including as unit testing, integration testing, functional testing, security testing, and user acceptability testing, were put to use. The application was fine-tuned with the support of regular contact with the development team as well as input from users, which helped to guarantee that it fulfilled the requirements and expectations of users. The Android application for Image Steganography provides a useful instrument for safe and private communication as a result of the project's success in accomplishing its goals. It gives people the ability to successfully safeguard their sensitive information, so preserving their privacy and keeping their confidentiality. The intuitive user interface and powerful security features contribute to the increased use and understanding of steganography as a dependable means for covert communication. Steganography may be used to hide information. Moving ahead, the application is capable of receiving more improvements and adjustments that may be done.

This involves broadening the scope of methods used in steganography, including more encryption algorithms, and putting in place improved security precautions. Continuous monitoring and upgrades will assist address newly discovered security threats, so ensuring that the application continues to be resilient and safe. In conclusion, the Android application that was built offers a helpful answer to those who are interested in securing their communication via the use of picture steganography. The programme gives users the ability to successfully safeguard their sensitive information by combining encryption and steganographic methods. This contributes to a heightened feeling of privacy and security in the era of the digital revolution.

AUTHORS' CONTRIBUTION

Author 1 and 2 implemented the concept and drafted the article with assistance of authors 3, 4 and 5, respectively. The author 6 and 7 reviewed the article.

CONFLICT OF INTEREST

The authors declare that have no competing interest.

REFERENCES

[1] Comparative study of image steganography techniques, Himanshu Arora, Cheshta Bansal, Sunny Dagar, International Conference on Advances in Computing, Communication Control and Networking, 2018, 982-985

[2] Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques, Srushti S Yadahalli, Shambhavi Rege, Reena Sonkusare, IEEE, 2020 ,1325-1330

[3] Review paper on image steganography, Deepali V. Patil, Mr. Shatendra Dubey, international journal of research in computer applications and robotic, 2014, Vol-02, 35-40

[4] Image Steganography: A Review of the Recent Advances, nandhini subramanian, omar elharrouss, somaya al-maadeed, ahmed bouridane, IEEE, 2021, Vol-9, 23409-23423

[5] Image steganography using lsb algorithm, Avni Aggarwal, Arpit Sangal, Aditya Varshney, International Journal of Information Sciences and Application, 2019, Vol-11, 85-89

[6] Enhancing Security of Image Steganography Using Visual Cryptography, Muhammad Aminul Islam, Md. Al-Amin Khan Riad, Tanmoy Sarkar Pias, 2nd International Conference on Robotics,Electrical and Signal Processing Techniques , IEEE , 2021 , 694-698

[7] Image Steganography Techniques - A Review Paper, Mohammed A. Saleh, International Journal of Advanced Research in Computer and Communication Engineering, 2018, Vol-7, 52-58

[8] Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB, Yani Parti Astuti, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, International Conference on Information and Communications Technology, 2018, 191-195

[9] Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones, Richard Apau, Clement Adomako, International Journal of Computer Applications, 2017, Vol-164, 13-22

[10] Stego App: Android based Image Steganography Application using LSB Algorithm, Azmat Ullah1, Mohsin Ijaz2, International Research Journal of Engineering and Technology, 2018, Vol-5, 862-865

[11] An Introduction to Image Steganography Techniques, Alaa A. Jabbar Altaay , Shahrin bin Sahib , Mazdak Zamani , International Conference on Advanced Computer Science Applications and Technologies , 2012 , 22-126

[12] Information Hiding in Images Using Steganography Techniques, Ramadhan Mstafa1, Christian Bach2, ASEE Northeast Section Conference, 2013, 1-8

[13] A secure steganography creation algorithm for multiple file formats, R. Vinothkanna, Journal of Innovative Image Processing, 2019, Vol-1, 20-30.

[14] Mohanaprakash, T., Subedha, V., & Lakshmi, D. (2015). Assisting
echolalia (Repetitive speech patterns) in children with autism using android mobile app. International Journal of Advanced Information and Communication Technology, 12(1), 928–933.

[15] Andavan, M.T., Vairaperumal, N. Privacy protection domain-user integra tag deduplication in cloud data server(2022) International Journal of Electrical and Computer Engineering, 12 (4), pp. 4155-4163.

[16] Mohanaprakash, T.A., Nirmalrani, V. Exploration of various viewpoints in cloud computing security threats (2021) Journal of Theoretical and Applied Information Technology, 99 (5), pp. 1172-1183.

[17] Andavan, M.T., Vairaperumal, N. Cloud computing based deduplication using high-performance grade byte check and fuzzy search technique (2023) Journal of Intelligent and Fuzzy Systems, 44 (2), pp. 3411-3425. doi: 10.3233/JIFS-220206

[18] N. Dudiki, S. Sangeetha, A. Manna, R. Pokhariyal, T. A.Mohanaprakash and A. P. Srivastava, "A Hybrid Cryptography Algorithm to Improve Cloud Computing Security, 2022