



BIOMETRIC DATA TRANSMISSION USING REVERSIBLE DATA HIDING FOR ENCRYPTION

¹Sajath S Chacko, ²Aathmana Aswini, ³Albin K Binu,
Yadhu Krishnan, Prof. Usha Gopalakrishnan

¹B. Tech Student, ²B. Tech Student, ³B. Tech Student, B. Tech Student, Associate professor

¹Department of Computer Science Engineering,

¹Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India

Abstract: Because the world is shifting its perspective on security and favouring biometric security over conventional passwords, the protection of biometric data is one of the most crucial security goals of the modern day. The emphasis is placed heavily on the use of arithmetic encoding for the compression of embedding data, and it is crucial to use a variety of biometrics rather than relying solely on one. It is suggested to transmit biometric data securely using block-by-block reversible encryption. Block wise encryption provides a high embedding space for the compressed biometric data as compared to other methods. The lossless arithmetic encoding approach not only allows for total reversibility but also precise secret data extraction and lossless image restoration. A substantial amount of data gathered through various comparisons can be used to support the notion that data compression and biometric data embedding rates can be significantly raised and can indicate successful working. Biometric data is encrypted to prevent unauthorised parties from accessing it, and the embedding of additional data is made possible by the lossless compression process of arithmetic encoding. The biometric data may be hidden in an image and stored in a database that is only accessible with a key that may be used to decode and extract the data without compromising the image's low efficacy or causing any data loss.

Keywords - Steganography, Cryptography, AES encryption standard, Biometric Data, Arithmetic Encoding.

CHAPTER 1

INTRODUCTION

Data Reversibility, The field of concealing is one of the most devoted to data protection through concealment. By simultaneously encrypting the image and masking the data, it enables the secret data to be integrated in the image using encryption. Only by employing a key to decrypt the encrypted image can the data be retrieved. A method for making sure a person is who they say they are is authentication. Through biometric authentication, which looks at biological features, this verification is carried out. An authentication system works by comparing the provided data with verified user information stored in a database. In traditional systems, this information is referred to as a password. In biometric authentication, information is referred to as bodily characteristics. Biometric information is unique from other security measures in that, if lost, it cannot be recovered because we cannot change our biometrics over the course of our lives. Biometric information is frequently stored in databases, which share the same security threats as other networking systems. This means that strong authentication must be in place in order to prevent unauthorised users from gaining access.

Over the past ten years, Reversible Data Hiding—where data is embedded in a picture but may still be retrieved together with the original image—has gained widespread recognition in the cybersecurity industry. Because the communication network and database where the information is stored both need legitimate and effective protections to secure them as they are most at danger, security has become one of the most important parts of biometric data transmission and storage. Privacy and authentication challenges must be overcome by security solutions. Due to the regular nature of these attacks on the network and database, data hiding techniques are used to safeguard the genuine data.

CHAPTER 2

LITERATURE SURVEY

2.1 Reversible Data Hiding, 2006:

Explored by Gaurav Sharma and Eli Sabre An innovative technique for lossless (reversible) data embedding (hiding). The approach is stated as having high embedding capacities, complete recovery of the original host signal, and little perceptible distortions between the host and picture containing the embedded data. The capacity of the scheme depends on the statistics of the host image. The machine has enough processing power to handle the vast majority of applications for typical photos. To vary the embedding level and trade off intermediate distortion for increased capacity, the technology can be modified for applications that call for high capacities. The generalised LSB embedding proposed in the current study significantly outperforms conventional LSB embedding algorithms in such cases because it gives finer granularity throughout the capacity distortion curve.

2.2 A Generalized Image Imploration Based RDH Scheme with HEC and IQ, 2014

Yuan Yu Tsai and Chi Shiang Chan present a generalised imploration-based RDH scheme. This paper proposes a novel, reversible picture interpolation-based data concealing technique. The recommended method achieves a high embedding capacity while maintaining a respectable level of image quality. The combination of the enhanced pixel mapping methodology and bilinear interpolation algorithms allows the proposed method to support magnified images at any resolution. The cover image's boundary region artefacts have also been eliminated concurrently. A superior pixel correction method was also applied to greatly enhance the image quality. In order to increase the embedding capacity, the Generalised Image Interpolation-based Reversible Data Hiding Scheme is changed. The outcomes of the studies show that our approach for reversible data concealing based on image interpolation is viable. The usage of high-dynamic-range photographs or 3D models as cover material can be facilitated by further research that builds on the interpolation techniques. There are several additional data embedding methods that improve image quality.

2.3 Reversible Data Hiding in Encrypted Image, 2015

An approach for Reversible Data Hiding in an Encrypted Image is presented by Anitha Hansoor and Prakash Pattan. Data extraction, data integration, data manipulation, and image encryption are the four phases involved in this. The content owner encrypts the cover image using an encryption key. The owner of the data enters information using the text or image that has been encrypted. The encryption key is securely obtained by the recipient via an appropriate key exchange protocol built on the RSA technique. The virtual embedding of information is carried out by the data manager, who also generates the data extraction key and extracts the pixel indices that correspond to the data bits. This extraction key is sent to the receiver after being encrypted with the RSA public key. If the recipient possesses a data extraction key, the original data can be obtained. A separable and reversible data masking technique is presented in the paper. In other words, the virtual embedding is performed after the data bits have been updated. The content owner uses an encryption key to first encrypt the cover image. Without knowing what was in the original image, Data Hider embeds the data using this encrypted image. Specific pieces of data are converted using MLSB technology. The modified information is combined with the image using virtual integration technology. After insertion, a data extraction key is produced, encrypted, and given to the receiver. Only the original image can be retrieved if the receiver only has the encryption key and the stereo image. Only if you also have the data overwrite key will you be able to import the original data from the stego photo. If you have a stereo image, the data extraction keys, and the encryption keys, you can import both the original image and the data. As a result, there will be a separation at the receiver side, and the receiver will be able to obtain information using the keys that are at their disposal. Only the LSB of the pixel is considered to have a virtual embedded in this article. For virtual data embedding, future advancements might include the LSB component of RGB components.

2.4 Biometric Security Based on RDH with RZL Code and ECC, 2015

Dr M Gobi and R Sreedevi suggests a person's personal secret information "m," which is to be stored in a secure manner, should be encrypted using Elliptic Curve Cryptography, an efficient asymmetric cryptosystem that uses both private and public keys to enable the secure data to be encrypted and produce the cypher text. The encrypted data "e" is placed within the user's biometric data, such as their fingerprints, iris, or even a photograph of their face, using RZL Coder, which in turn uses a histogram pair-based image concealment approach. This cover biometric image is stored on a public server after embedding, making it a great target for multiple attackers. The encrypted data "e" is placed within the user's biometric data, such as their fingerprints, iris, or even a photograph of their face, using RZL Coder, which in turn uses a histogram pair-based image concealment approach. This cover biometric image is stored on a public server after embedding, making it a great target for multiple attackers. After extracting his encrypted personal information from his biometric image for authentication, the user uses RZL Decoder to recover both the original biometric image and the encrypted data. The data is subsequently encrypted using ECC Decryption in order to recover the original information, which is incredibly confidential to that person. The incredibly secure asymmetric cryptosystem ECC is used in this method to keep the data from intruders.

Their capacity to distinguish between authorised people and imposters or those who unlawfully get the access privilege of an authorised person makes them more popular than traditional identifying systems. However, there are serious concerns over the reliability and security of the biometric data themselves. Steganography, watermarking, and encryption are all workable solutions for the protection of biometric data. In this paper, two techniques for protecting such data with steganography and cryptography are presented. In addition to image concealment, encryption is another technique for strengthening the security of biometric data. Enhancing the security of steganographic-based biometric data sharing is the first application. In the second application, we mix thumb impressions and fingerprint photos. To avoid the fingerprint matching features being drastically altered during encoding and decoding, the data is concealed in this application. The accuracy of the verification based on decoded or embedded images is as accurate as that of the original images as a result. The host pictures' ability to conceal data is currently being enhanced.

2.5 Multi-Level Reversible Data Hiding Using LSB Based Steganography, 2018

Here, C. Dharani and K. Jaspin study steganography. The main cover media in this essay are images. There are two further steganographic-related technologies: fingerprinting and watermarking. This concept just uses the least significant bit of the alpha channel of a pixel. There are no changed colour values in this picture. Before the message can be embedded, the image must contain the message's length. The first 32 pixels are utilised to extract bit number 0; to calculate the size of the message that is embedded in the image, the bits must be properly placed inside an integer variable. The pixels that follow the 32nd pixel contain the bits needed to produce the byte value needed to create the original string. The LSB replacement approach is used at the sender side to initially embed the secret data into the original image. Thus, a stego-image is produced. A new cover image has been selected to hide the Stego-image. As a result, the use of several encryptions here increases security. The picture that was received from the sender must first be decrypted in order for the receiver to retrieve the Stego-image. Decrypting the stego image yields the original hidden message. In this suggested architecture, we have employed multilevel encryption to boost security and LSB techniques to embed data into the image. The embedding capacity could be increased further by future additions of new modules.

2.6 Secure Biometrics Using Difference Expansion RDH Techniques, 2018

Farah Shah Khan and Shivani Gupta explore the scenario in which a cover image has an embedded raw or processed fingerprint image. This process involves inserting biometric information or an image of a fingerprint onto the cover image of choice using a variety of expansion techniques, and then encrypting the image with cypher keys. The encrypted image is currently being broadcast over the internet. On the receiving end, data is first decrypted, and the receiver uses the DE bit recovery process to receive error-free data. This data transfer can take place over any secure network, including fibre optic networks, GPS/GPRS, and others. It is obvious that the size of the selected cover image must be sufficient to include both data and a location map bits. Before implantation, each fingerprint is processed independently. However, anyone may use a stage image before embedding. As we transfer photographs early, the recipient will require more time. However, this example uses the approach that is the most successful. Minute points are selected from the fingerprint picture that was obtained at the receiver. These minute particulars are then used to create a map, and the data is ultimately transformed into a stream of data. The difference expansion approach is a reversible, error-free data concealing technique.

2.7 LSB Based Text and Image Steganography Using AES Algorithm, 2018

Priya Paresh Bandekhar and Suguna G suggest a study about the LSB technique (LSB), which involves embedding the secret data into the cover image in order to conceal the imager using the LSB algorithm. AES (Advanced Encryption Standard) is used to protect and provide security for the stegoimage. The secret data is concealed in the cover image using numerous images in a variety of formats. Then the difference between the original and encrypted image's PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) are estimated. Plotted are PSNR, MSE, and histogram.

the practise of employing the LSB method to conceal sensitive information, such as a word or image. Additionally, the AES technique is used with a maximum key length of 128 bits to provide and safeguard the data. Software called MATLAB implements image steganography.

CHAPTER 3

3.1 ALGORITHMS

AES Algorithm

As a result of its reputation for security, the AES algorithm has become a global standard. The AES method uses a substitution permutation (SP) network with several rounds to produce cypher text. The key size determines how many rounds there will be. A 128-bit key size, 192-bit key size, and 256-bit key size determine the number of rounds in ten, twelve, and fourteen, respectively. Each of these rounds needs a round key, but since the algorithm only accepts one key, it must be expanded to obtain keys for every round, including round 0.

The algorithm has four steps in each round.

1. Byte substitution: In the first phase, the block text's bytes are substituted in accordance with guidelines set forth by predefined S-boxes (also known as substitution boxes).
2. Rows shifting: The permutation stage is the next. All rows other than the first are relocated by one in this phase, as displayed below.
3. combining the columns: The third step of the Hill cypher involves combining the columns of the block to further muddle the message.
4. Adding the round key: The message is XORed with the appropriate round key in the last step.

These stages, when repeated, guarantee the security of the final ciphertext.

LSB Algorithm

The simplest approach for encoding secret information is the Least Significant Bit (LSB) method. The secret information can be concealed in pixels by replacing the minimal weighting value of a bits of the pixel with binary bits of secret information data. Only extracting secret information bits from the corresponding locations serves as a function in the receiver. A pseudorandom sequence can be used to choose the location where the secret binary information will be embedded, which will make it harder to detect secret data. The LSB approach has a high hiding capacity, is straightforward and simple to use, and embeds and removes information quickly despite its lacklustre security.

This method encrypts a message by altering the final few bits of a byte. It works particularly well in situations where red, green, and blue values for each pixel in a picture are represented by three different colours. Eight bits, or one byte, are used to represent

values ranging from 00000000 to 11111111 in binary or 0 to 255 in decimal. Consider an 8-bit red pixel. Encoding data into the image is possible by changing the last two bits of a completely red pixel from 11111111 to 11111101, which changes the red value from 255 to 253, which is essentially imperceptible to the unaided eye.

CHAPTER 4 EXISTING SYSTEM

This research introduces a secure system for sending biometric data in a cloud-based environment. We used multifactor authentication, such as face and fingerprint recognition, to demonstrate the entire project there. The feature matching of biometric data will take place in a cloud service provider in such a case. A significant concern is the safe transfer of fingerprint and face image information from client to server. To hide the fingerprint information in the coloured face photos during the image encryption process, a reversible data hiding architecture based on encryption is introduced in this manuscript. The suggested approach offers the ability to transmit an encrypted face image that contains fingerprint information.

Reversible data hiding algorithm, picture recovery, and biometric data extraction algorithms are all described and are used throughout the strategy. The procedures used for the reversible data concealing process are shown in Algorithm 1. Algorithm 2 shows the extraction of biometric information as well as the lossless extraction of our facial image. The method is shown in Algorithm 3 measures the smoothness of the picture. In order to verify that our face picture is accurately recovered, Algorithm 2 must compute a smoothness measure algorithm that examines the naturalness property of an image block, in this instance the face image. For data concealment, the user will have an encryption key called K. By executing bit-wise XOR operations () between the blocks of the pseudorandom matrix created by utilising the encryption key K and the blocks of the original face picture, the face image will be encrypted.

CHAPTER 5 PROPOSED SYSTEM

Image steganography project is used to hide biometric data using RDH in which we are hiding in the image using encoding and decoding functions and compressing a series of biometric data through arithmetic encoding. We are creating an android app in which there are login and registration pages, once you logged in you get two buttons : Encrypt and Decrypt

- For Encryption, Enter a name for the secure data, select any biometric data, then a random key would be generated and then the email id of the recipient. The data would be encrypted into an image and sent to the receiver
 - The image in which the encrypted data is hidden would also be encrypted and in .png format.
 - Encrypted hidden image would be sent to the receiver's email with the random key.
 - The encryption of both the data and the image would be done using AES 256.
- For Decryption, select the encrypted image to be decrypted, type in the random key and thus the biometric data can be viewed. Both the sender and receiver need to be registered and using the android app.



5.1 SYSTEM ARCHITECTURE

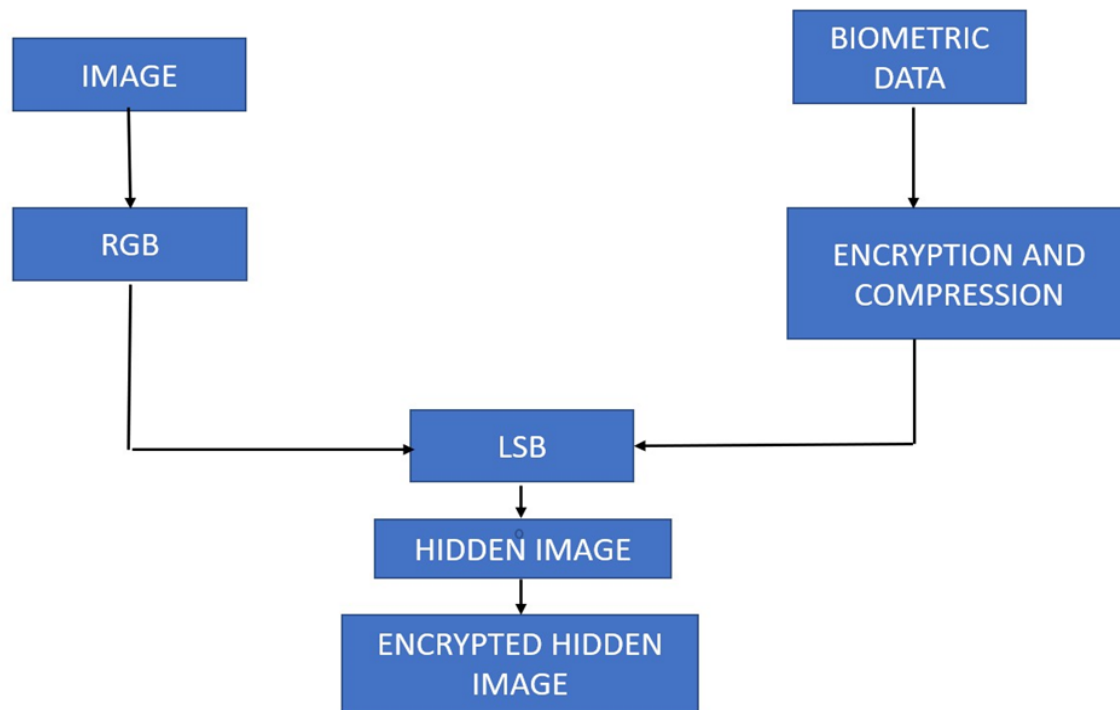
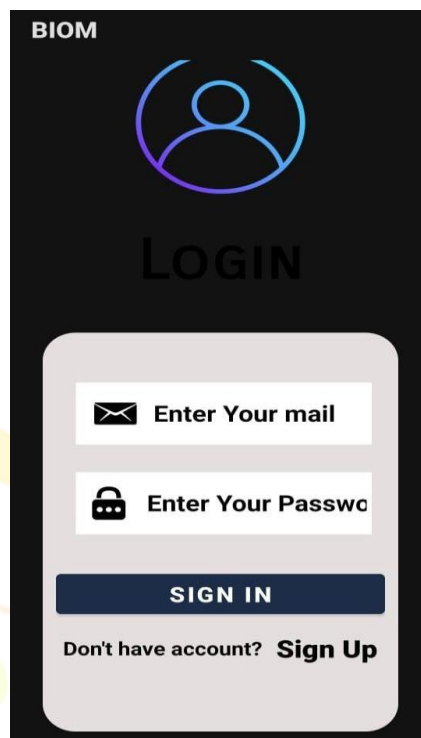


Fig 5.1.1 : Block Diagram of the system



CHAPTER 6 MODULES

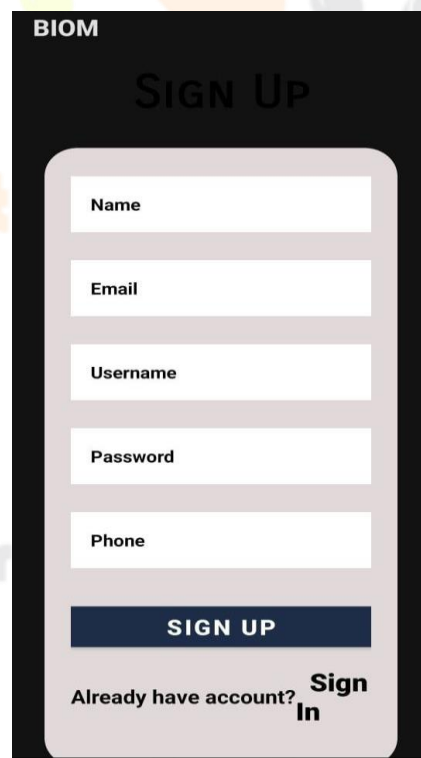
6.1 Login Page



The login screen for the BIOM mobile app features a dark background. At the top, the word "BIOM" is displayed in white. Below it is a blue circular icon representing a user profile. The word "LOGIN" is centered in large, bold, white letters. A light gray rounded rectangle contains the login form, which includes two input fields: "Enter Your mail" with an envelope icon and "Enter Your Password" with a padlock icon. Below these fields is a dark blue "SIGN IN" button. At the bottom of the form, the text "Don't have account? Sign Up" is displayed, with "Sign Up" in bold.

Fig. 6.1.1: Sign in Page

6.2 Registration Page



The registration screen for the BIOM mobile app has a dark background. At the top, "BIOM" is written in white, followed by "SIGN UP" in large, bold, white letters. A light gray rounded rectangle contains the registration form with five input fields labeled "Name", "Email", "Username", "Password", and "Phone". Below these fields is a dark blue "SIGN UP" button. At the bottom, the text "Already have account? Sign In" is shown, with "Sign In" in bold.

Fig. 6.2.1: Registration Page

6.3 Sender / Receiver Page



Fig. 6.3.1: Send and receive the encrypted data

6.4 Encryption / Senders Page

 A mobile application interface for sending encrypted data. At the top, a black header bar contains the text 'BIOM'. Below it is a dark blue navigation bar with the word 'Encrypted'. The main content area has a white background and contains several input fields and a submit button. The fields are labeled 'file name', 'email', 'AES Security Key', and 'file'. The 'file' field includes a 'Choose File' button and the text 'No file chosen'. A green 'Submit' button is at the bottom. The background features a faint, colorful logo with the text 'International Journal of Novel Research and Development' and 'Innovation'.

Fig. 6.4.1: Encrypt the biometric data

6.5 Decryption / Receivers

BIOM

Encrypted

DECRYPTION

AES Security Key

Choose File

No file chosen

Submit

Fig.6.5.1 Decrypt the encrypted hidden image

6.6 Original Image



Fig.6.6.1 Original Image

6.7 Encrypted Hidden Image

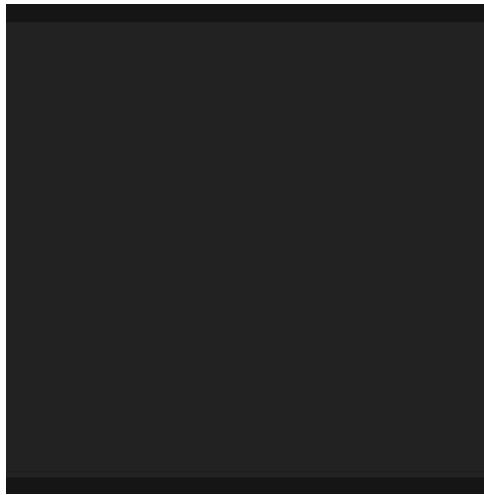


Fig 6.7.1 Encrypted Image

6.8 Decrypted Image

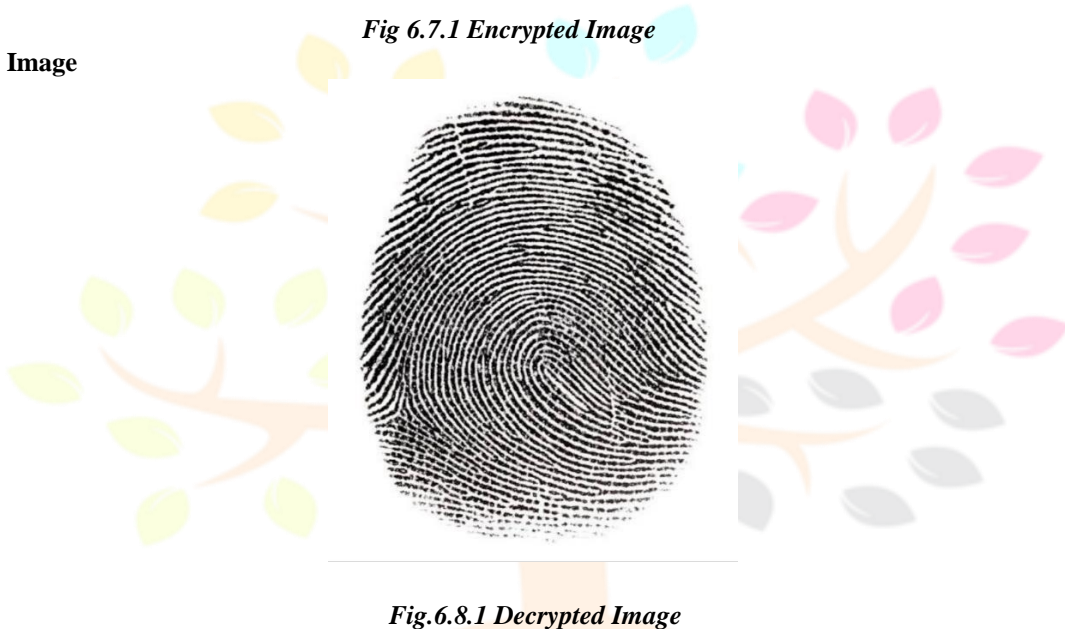


Fig.6.8.1 Decrypted Image

CHAPTER 7 CONCLUSION

In a image steganography, we utilise encoding and decoding techniques to conceal a secret message inside an image. The approach of reversible data concealing is suggested in the paper. In other words, the data bits are modified before virtual embedding and the virtual embedding is carried out. The confidential data is initially encrypted by the sender using an encryption key. LSB method is used to insert the transformed data into the image and create a stego image. A data extraction key is generated after insertion. The entire image is then encrypted using an encryption technique and an encryption key. Here, a stego image that is encrypted is created. The addressee receives this encrypted stego picture. The operation is reversed at the recipient side compared to the sender side, using the decryption key, the receiver must first decrypt the encrypted stego picture. Then, the stego image is used to extract the encrypted data. Using the decryption method and the decryption key, the original secret data is finally unlocked. This confidential information is used by the receiver and stored for later processing. As a result, the idea offers a practical method for leveraging the LSB and AES algorithms to hide and retrieve data.

ACKNOWLEDGMENT

We would also want to express our sincere gratitude to our department head, professor Usha Gopalakrishnan, and our project advisor, professor Usha Gopalakrishnan, for their help and advice in making this research feasible. Their invaluable advice, from the very beginning to the very end, enabled us to finish this study report. We sincerely appreciate the assistance of all the faculty members who provided us with helpful guidance and made the completion of this task simple.

REFERENCES

- [1] “A New Framework for secure biometric Transmission using Block-wise Reversible Data Hiding Through Encryption” V.M.Manikandan ,Harshad Dhane .2021
- [2] “Reversible Data Hiding” by Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su. .2016.
- [3] “Encryption of Gray Images using Scalable Codes” by Pooja Bhat and P. K. Ajmera. 2014.
- [4] “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption” by Kede Ma, Weiming Zhang, Xianfeng Zhao, Member,2013.
- [5] “Reversible Data Hiding” Gaurav Sharma, Eli Saber (2006)
- [6] “Reversible Data Hiding in Encrypted Image” Anitha Hansoor, Prakash Pattan (2015)
- [7] “Biometric Security based on RDH with RZL code and ECC”, Dr M.Gobi , Mrs R.Sreedevi (2015)

