Secure Data Hiding & Data Encryption Over Image Steganography via Key Modulation

M.Krishnamoortyhy [1], Dr.N.Pughazendi [2], S.Yoga Dinesh[3]S.Vignesh [4], R.Vighneshwaran [5] , B.Jabir Ahmed [6].

[1] Associate Professors,Computer Science Engineering, Panimalar Engineering College Chennai,Tamil Nadu,India
[2] Professors,Computer Science Engineering, Panimalar Engineering College Chennai,Tamil Nadu,India
[3] Associate Professors,Computer Science Engineering, Panimalar Engineering College Chennai,Tamil Nadu,India
[4] Student,Computer Science Engineering, Panimalar Engineering College Chennai,Tamil Nadu,India
[5] Student,Computer Science Engineering, Panimalar Engineering College Chennai,Tamil Nadu,Indi
[6]Student,Computer Science Engineering, Panimalar Engineering College Chennai,Tamil Nadu,India

ABSTRACT

This application helps you to insert or hide necessary or personal messages or files into files like footage, audio and video whereas not touching the standard of actual files. It achieves this by exploitation the tiniest amount necessary bits of those files for embedding information that don't seem to use by the Image viewers or Image editors. The data embedding is achieved through a public key modulation mechanism, at intervals that access to the key secret writing key's not required. At the decoder aspect, a strong two-class SVM classifier is supposed to differentiate encrypted and non-encrypted image patches, allowing U.S. to conjointly decipher the embedded message and then the primary image signal. Compared with the state-of-the-arts, the projected approach provides higher embedding capability, and is in an extremely position to fully reconstruct the initial image besides as a results of the embedded message. It permits you to insert the messages or files in encrypted type exploitation steganography and uniform embedding formula that suggests that once encrypted, the message or file is also retrieved (or decrypted) from a data file alone once specifying the right secret that was used at the time of secret writing. It permits embedding messages and files in compressed type exploitation amount compression format. Provides you a spread of compression level to be used- low, ancient or high. The Internet as a full doesn't use secure links, therefore data in transit is to boot in danger of interception to boot. the obligatory of reducing an opportunity of the knowledge being detected throughout the transmission is being a haul presently days. The projected theme gains favorable performance in terms of secure embedding capability against steganalysis Some resolution to be mentioned is that the because of passing data throughout a} manner that the terribly existence of the message is unknown therefore on repel attention of the potential aggressor. Be sides concealing information for confidentiality.

IndexTerms— *information concealing, key stream, Image secret writing,*

1. INTRODUCTION

This system is employed to create a secured transmission of messages, files over anyplace through LAN or WAN .In this system we have a tendency to used the construct known as STEGNOGRAPHY[1-6] and also the Technique used BPCS(Bit Plane Code Segmentation).Here it's achieved by concealing the data into the carrier file.The formats supported for the image during this system square measure jpg png, tiff. In this system we used three different types of carrier files they are Images, Audios and Videos.

- The formats supported for the image in this system are jpg , png , tiff.
- The formats supported for the audio in this system are mp3, wav.
- The formats supported for the video in this system are avi, mpeg.

This project mainly focuses on the data security mostly used in military fields **for example**, During World War II, a spy for the Japanese in New York City, Dickinson, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed how many of this or that doll to ship. The stego text was the doll orders, the concealed 'plaintext' was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.

2. KEY FEATURES

Our project has the following key features,

- Encryption
- Compression
- Decryption
- Decompression

2.1 ENCRYPTION/DECRYPTION

Encryption is that the method of remodeling data (referred to as plaintext) exploitation associate degree formula (called cipher) [4] to form it undecipherable to anyone except those possessing special data, typically cited as a key [1]. The results of the method is encrypted data (in cryptography, cited as cipher text) **Decryption** is that the reverse method of the coding.

2.2 COMPRESSION/DECOMPRESSION

Compression is that the art or Science that represents data in an exceedingly compact type. Compression is that the method of reducing the scale of a file [1]. The aim of information the information compression is to cut back redundancy in keep or communicated data, therefore increasing effective knowledge density [4]. **Decompression** is that the reverse method of the compression

3. SYSTEM STUDY

3.1 EXISTING SYSTEM

Previously we've used a system that solely hides the data within the main file and it supports solely few formats of master files [1]. This method doesn't support the cryptography and additionally compression. Here we will hide solely the message and it won't supports concealment of files. The system used earlier solely Supports the cryptography [7] which means it simply protects the file by providing a countersign. And additionally the previous system supports solely bytes of knowledge to cover [5] .There is no system that supports every kind of multimedia system files as main file. Existing systems affects the insufficient bit originality of main file and also the overall method is small bit complicated, consumes a lot of time.

DISADVANTAGES

Message is difficult to recover if image is subject to attack like translation and rotation.Significant harm to image look. Message troublesome to recover.Relatively simple to discover, as our project has shown.Image is distorted. Message simply lost if image subject to compression like JPEG.

3.2 PROPOSED SYSTEM

In this projected system we tend to square measure getting to embedded each the message and get into the computer file. Our system supports several formats of the master files like image, audio and video files and conjointly our system supports each the encoding and compression. It conjointly supports great deal of knowledge to be embedded. This system won't have an effect on the originality of the file and our system is user friendly therefore the overall method may be created simply. It conjointly uses terribly powerful encoding and compression rule. This system provides a lot of confidentiality and authentication. sepulchre analysis is tough in our system due to the powerful rule and length of the countersign.

ADVANTAGES

Hard to notice Original image is extremely the same as altered image.Embedded knowledge resembles Gaussian noise.Hard to notice as message and elementary image knowledge share same vary.Altered image closely resembles original.Not liable to attacks like rotation and translation.

4. LITERATURE SURVEY

"A Review on Steganography Techniques and Genetic Algorithm used in Information Hiding"

Approach based on heuristic genetic algorithm, which optimally find the appropriate locations in cover image to hide data. Simulation results show that their method is more efficient than traditional LSB based method. LSB algorithm improves high stego image quality. Least changes in the bits causes image corruption

"Improved FPGA based X-Box Mapping of an Image using Steganography Technique"

Authors present the data hiding method for color RGB images. X-box mapping is utilized for this purpose. Their system is more secure and provides higher values of PSNR.Very difficult for the attacker to extract the secret information because they make use of mapping. PSNR value is high. Encryption takes longer time. PSNR value which leads to greater stego image quality. X-Box mapping is used and several boxes contain 16 different values. Here "X" represent any integer number from 0 to 9.

"Reversible Data Hiding in Encrypted with Distributed Source Encoding"

Approach makes you embed or hide important or private messages or files into files like images, audio and video without affecting the quality of actual files. It achieves this by using the least significant bits of these files for embedding data which are not used by the Image viewers or Image editors. Hard to detect Original image is very similar to altered image. Message is hard to recover if image is subject to attack such as translation and rotation.The very existence of the message is unknown in order to repel attention of the potential attacker. Be sides hiding data for confidentiality.

"An improved LSB image steganography technique using bit-inverse in 24 bit colour image"

New steganographic method is proposed and implemented based on bit inversion. Experimental results represent that PSNR value of stego image is improved using this method. correct retrieval of secret messagemodification in pixelsApproach demonstrate that PSNR value of stego image is improved; hence stego image quality is improved.

"A Novel DWT based Image Securing method using Steganography"

New method has been proposed in which multiple RGB images are embedded into single RGB image using DWT. Proposed system has high embedding capacity and security with minimal changes in stegoimage. Proposed method has good level of PSNR and SSIM index values Supports few formats of images. So overall security of their approach is high with less perceptible changes in stego image.

"Image Steganography using LSB and LSB + Huffman Code"

Huffman coding based novel steganographic technique of LSB substitution. This work mainly focuses on high security and embedding capacity and acceptable level of visual quality of stego image. Experimental results demonstrate that proposed scheme has PSNR of 30 dB to 31 dB. very difficult for attacker to extract the secret information because Huffman table decrease the size of the cover image.PSNR values and lie between 30 dB to 31 dB. Approach focuses on high security, larger embedding capacity and acceptable level of stego image quality.

"A Novel Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images"

Authors proposed a new edge adaptive steganography based on LSB substitution. Experimental results show that this technique is efficient than LSB and other pixel differencing methods. quality of stego imageis high.differences adjacent pixels of carrier imageLSB and Pixel difference based techniques and maintains the quality of stego image.

"Random Image Stegano-graphy in Spatial Domain"

New image steganographic method is proposed based on LSB substitution method using random bit selection. Pixels are selected in random fashion for embedding based on intensity values, location of pixel and so on. Techniques based on random pixels of cover image and secret information is embedded in randomlyIndex values for encryption has high complexity**.**Selected bits of random pixels. Intensity values, location of pixels etc. parameters are used for this purpose.

"A High capacity data-hiding technique using steganography"

Proposed to a technique of information hiding in which adaptive steganography is used with RGB images to embed Data in all the channel to enhance the embedding capacity of the system. Simulation results show that proposed method has high embedding capacity. high embedding capacity than traditional LSB method and low computational complexity Sensitive information maintance is complex Approach system provides good quality of stego image.

"Image and Text Steganography Based on RSA and Chaos Cryptography Algorithm with Hash-LSB Technique"

In this projected work Chaos primarily based cryptography is employed with steganography. Chaotic provision and cat map ar used because the base for his or her image secret writing algorithmic program. Results demonstrate that projected system has zero.981 SSIM index price and forty seven.71 dB PSNR More efficient and secure against attacksGenerates very good quality of stego image and it is more efficient and secure against and can be used for real time image encryption and transmission. Encryption of data to image takes longer time Generates superb quality of stego image and it's a lot of economical and secure against attacks and might be used for real time image secret writing and transmission

"A Novel Secure Communication Protocol Combining Steganograp-hy and Cryptography"

Proposed a awfully innovative methodology that mixes the steganography and cryptography into one system. No separate. computations are going to be finished these 2. hence the new system desires only a few computations than existing techniques, whereas maintaining high security level. Simulation results show that this technique is safe from Steganalysis attacks, very much safer from steganalysis attacks, Does not provide higher security levels. Boolean functions area unit applied for cryptanalytic purpose and to regulate the pseudo-random increment and decrement of LSBs. Experimental results shows that this technique is extremely a lot of safer from steganalysis attacks.

5. ARCHITECTURE DIAGRAM

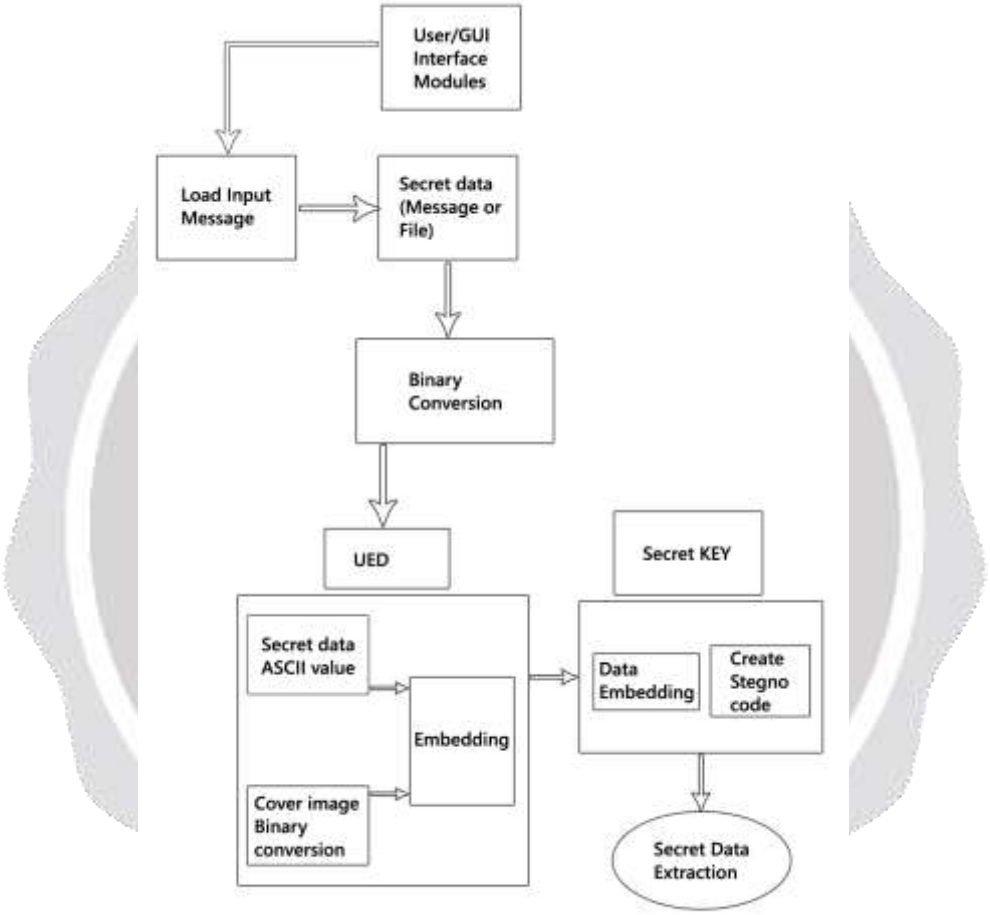


Fig-1:ARCHITECTURE DIAGRAM

6. IMPLEMENTATION

6.1 METHODOLOGY

ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES may be a cruciform key block cipher printed by the agency in Gregorian month 2001. Agency analysis criteria for AES are [1] Security [2] value [3] algorithmic program and Implementation Characteristics. AES may be a non-Feistel cipher that encrypts and

decrypts an information block of 128-bits. The key size will be 128,192 or 256-bits. It depends on variety of round the input of the encoding and coding algorithmic program may be a single 128-bit block. The block is diagrammatic as a row of matrix of sixteen bytes. AES structure isn't a Feistel structure .Encoding is that the method of changing plaintext to cipher-text (had to understand) by applying mathematical Transformation These transformation are referred to an encoding algorithms and need associate degree encoding key.

Coding is that the reverse method of obtaining back the first information from the cipher-text employing a coding key and therefore the coding key may be identical as in symmetric or secret key cryptography, The key will completely different as in uneven or public key cryptography.

6.2 HOW TO EMBEDD A MESSAGE

Click on 'Embed Message' button or select File engraft Message from the menu.Select the main file which is able to be used for embedding information into. Select the computer file which is able to contain the embedded message. This file are associate a replica of main file and can containing the embedded message. In the 'Embedding message' panel, Key within the message within the message box or paste a text already gift on the writing board. Choose the choices to be used whereas embedding message. These choices embody Compression and coding.

If you specify coding to be used, you will have to specify a parole that could be a minimum of eight characters long. You can modification the main file or computer file by clicking on 'Change' button next to every item. Finally once you are able to go, click on 'Go' button

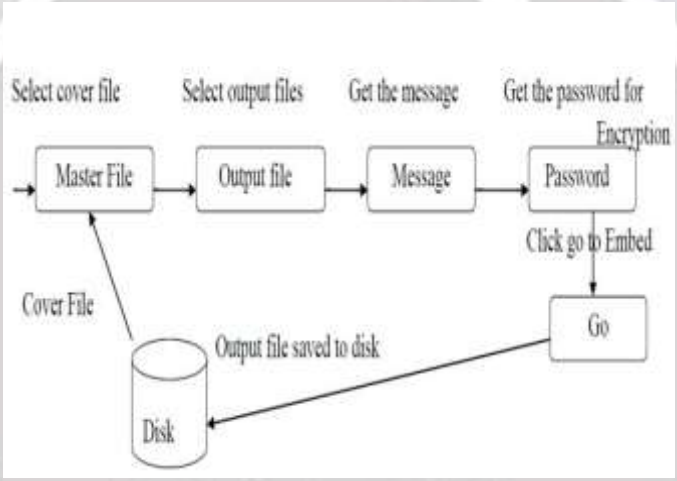


FIG-2:HOW TO EMBEDD A MESSAGE

6.3 HOW TO RETRIEVE A EMBEDDED MESSAGE

Click on 'Retrieve Message' button or opt for File Retrieve Message from the menu.

Select the main file containing the embedded message. A panel can seem summarizing the properties of the main file. it shows you whether or not the file contains Associate in Nursing embedded message or a file, Steganography version accustomed engraft the message/file, whether or not compression and secret writing are used and therefore the compression quantitative relation if compression has been used. It conjointly shows you the request you've got created. Finally once you are able to go, click on 'Go' button. If the message is encrypted, you'll be asked for the positive identification. Key within the positive identification and click on on the OK button.

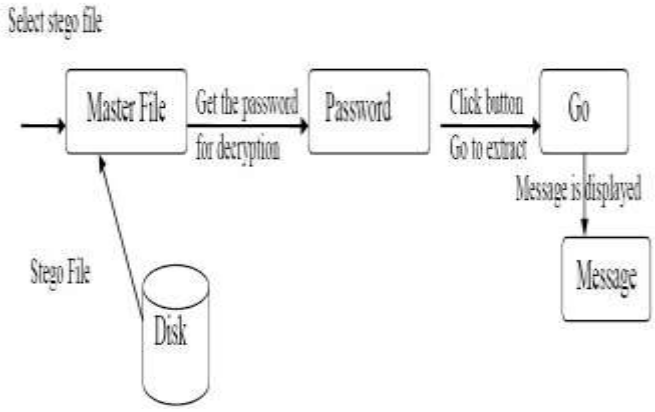


FIG-3:HOW TO RETRIEVE A EMBEDDED MESSAGE

6.4 HOW TO EMBEDD A FILE

Click on 'Embed File' button or select File imbed File from the menu. Select the main file which can be used for embedding knowledge into. Select the computer file which can contain the embedded file. This file are an a duplicate of main file and can containing the embedded file. Select the info file which can be embedded into the main file. In the "Embed file" window, select the choices to be used whereas embedding the info file. These choices embrace Compression and encoding. If you specify encoding to be used, you will have to specify a countersign that could be a minimum of eight characters long. You can modification the main file, computer file or file by clicking on 'Change' button next to every item. Finally once you are able to go, click on 'Go' button.

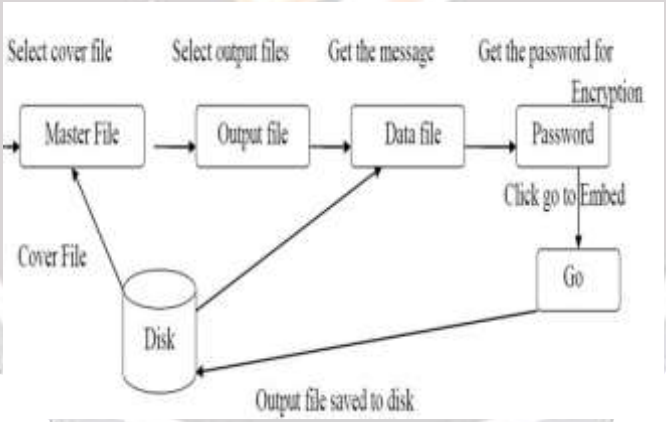


Fig-4:HOW TO EMBEDD A FILE

6.5 HOW TO RETRIEVE A EMBEDDED FILE

Click on 'Retrieve File' button or opt for File Retrieve File from the menu. Select the computer file containing the embedded file. A panel can seem summarizing the properties of the computer file. it shows you whether or not the file contains associate embedded message or a file, Steganograph version accustomed plant the message/file, whether or not compression and cryptography are used and also the compression magnitude relation if compression has been used. It additionally shows you the request you've got created. Finally once you are able to go, click on 'Go' button. If the file is encrypted, you'll be asked for the watchword. Key within the watchword and click on on the OK button. The file are retrieved and keep in current operating directory. If it's detected that you simply square measure employing a Windows platform, you'll have a option to open the file directly from the appliance.

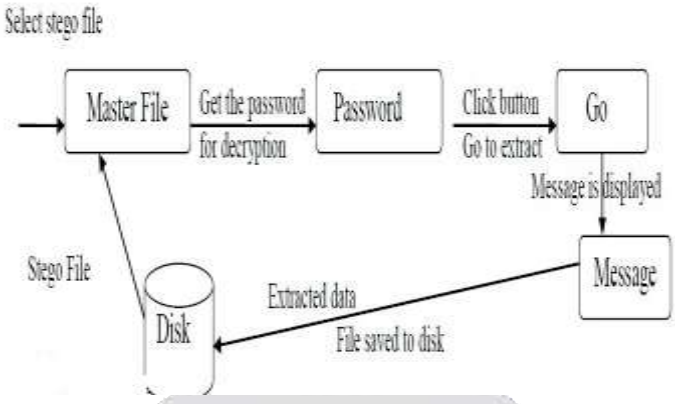
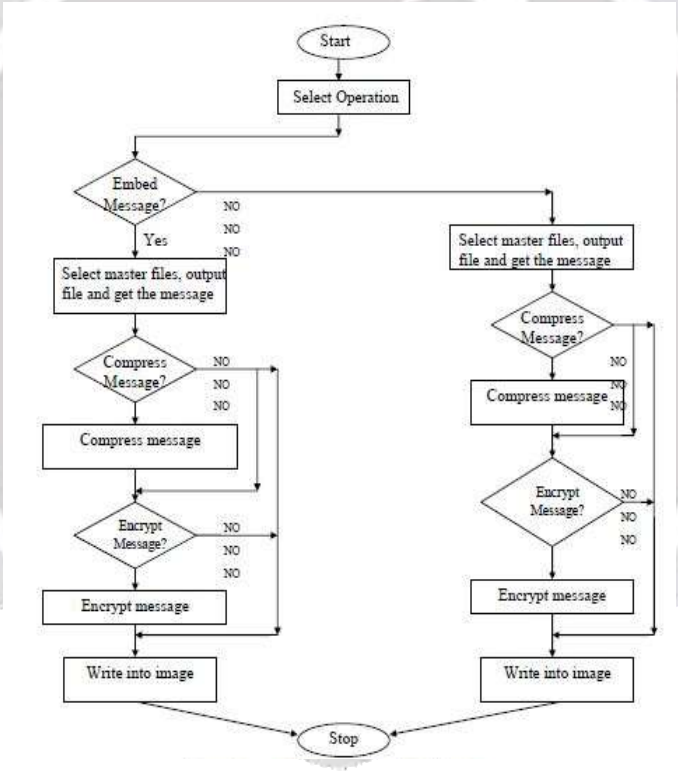


Fig-5: HOW TO RETRIEVE A EMBEDDED FILE

6.6 FLOWCHART



In this concept user need to select the option like embed a message, Embed a file, Retrieve a message, Retrieve a file. For each and every option has a some constraints like choosing the image, and a file which is to be embedded into image, the every embedded file has need to set a key for security. While decryption or retrieval of data need the secret key which is set at a encryption or embedded time, if the secret key is not valid at the time of retrieval the data which is embedded cant retrieved.

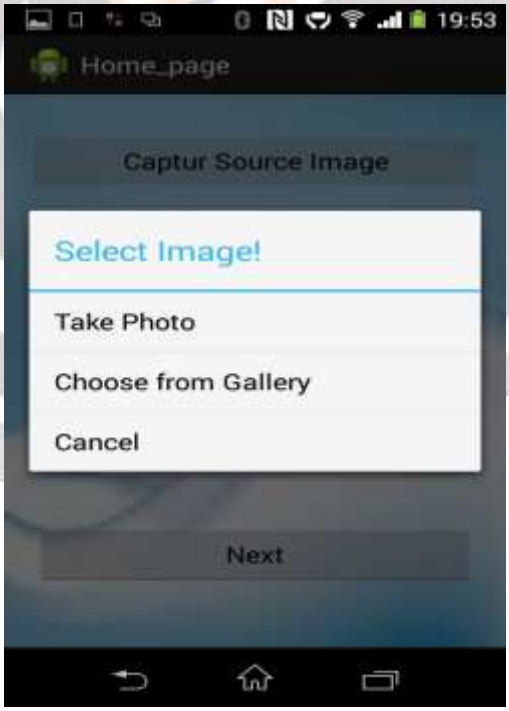
7. RESULTS & DISCUSSIONS

In this activity the user has to enter the registered username and password for validation.

Before login in, user need to register in the registration in this activity. After registration the user data will be saved into the database.

These are the options available to perform image stegnography operations, embed message option use to embed a message into the image with a secret key. Embed file option use to embed a file like audio, video, pdf, rar, word, excel, and some other files can be embedded into the image.

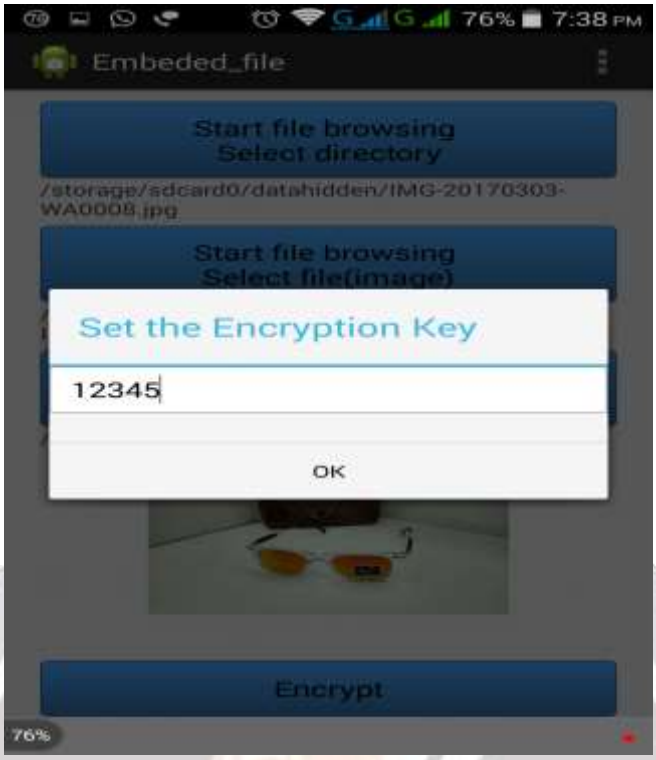
This is the default image used to embed a message



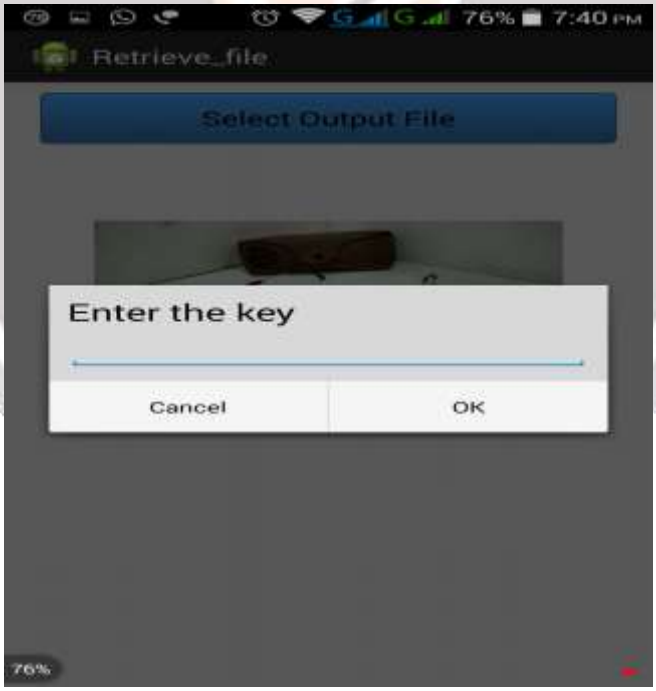
In this the user can choose the image using various options such as taking the photo and choosing the image from gallery.

After choosing the image the user have to enter the message. The user can also specify the The compression range. The compression value ranges from 0 to 10.

The user needs to enter 9digit Key to encrypt and Decrypt aimage. The user must send the key to the receiver. The receiver must enter the key to decrypt the message.



This activity is use to embed a file in a image. We need to set a encryption key to encrypt a file in to the image.



This activity used to retrieve a file from the master file (file which is embedded into the image).

8. CONCLUSIONS& FUTURE SCOPE

The planned framework is appropriate for the divisible reversible data-hiding theme in encrypted image, which might supply comparatively high payload and error-free information extraction. this method provides additional confidentiality and authentication used to form a secured transmission of messages, files over anyplace through LAN or WAN.

FUTURE SCOPE:

This software project is intended to provide the transfer of secret message m embedded in the image data 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 mind

9. LIST OF REFERENCES

[1] Fangjun Huang, Jiwu Huang, Yun Qing Shi*"* New Framework for Reversible Data Hiding in Encrypted Domain*"* *IEEE Transactions on Information Forensics and Security*, T-IFS-05917-2016

[2] Y. Qiu, Z. Qian, and L. Yu, "Adaptive Reversible Data Hiding by Extending the Generalized Integer Transformation," *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 130-134, 2016.

[3] Z. Qian, and X. Zhang, "Reversible Data Hiding in Encrypted Image with Distributed Source Encoding," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 26, no. 4, pp. 636-646, 2016.

[4] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing*, vol. 94, pp. 118-127, 2014.

[5] Z. Qian, X. Zhang, and S. Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream," *IEEE Trans. on Multimedia*, vol. 16, no. 5, pp. 1486-1491, 2014.

[6] Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," *The Scientific World Journal*, vol. 2014, pp. 1-9, 2014.

[6] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key," *IEEE Stegnography*, vol. 23, no. 1, pp. 130-134, 2011.

[8].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,

[9].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.

[10]. Suriyani Ariffin,Faculty" SMS Encryption using 3D-AES Block Cipher on Android Message Application" vol. 8, no 3, 2013.

BIOGRAPHIES

S.Vignesh
B.E., Computer Science and Engineering,
Panimalar Engineering College.

B.JabirAhmed
B.E., Computer Science and Engineering,
Panimalar Engineering College.

R.Vighneshwaran
B.E., Computer Science and Engineering,
Panimalar College Engineering College.