Development of Novel Algorithm for Data Hiding on Mobile Application

Roopesh Kumar, Ajay Kumar Yadav
Department of Computer Science
Banasthali Vidyapith, Newai Tonk, India

***Abstract*—We can easily observe that in the current era of communication, Computers, mobile phones, and the Internet are widely used mediums. In such an environment, information security is an important issue. The most common techniques used for information security are Cryptography and Steganography. Many research works have been done on image Steganography. These images have different kinds of formats like BMP, GIF, and PNG. Several compression methods are available which applied to the images having the format BMP, GIF, and PNG is comparatively less effective than the JPEG image. JPEG compression steganography method is complex to implement even then some algorithms have been developed for it. They provide single-level or two-level information securities. This paper presents a method in which is the combination of Cryptography and Steganography is used over android mobile phones. Here we are performing encryption two times on data to be hidden and then that encrypted data hidden both in text and image. We are using the Advanced Encryption Standard (AES) algorithm to hide text within a text, Discrete Cosine transform (DCT) for image steganography, and Data Encryption Standard (DES) for encryption of text. This paper gives the idea of three-level information security over the android environment.**

***Keywords*—Steganography encryption; discrete cosine transform; DES; F5Algorithm**

I. Introduction

Information security is a popular research area. It attracted researchers towards the security concept of data by using different kinds of techniques. The commonly used are Steganography, watermarking, and cryptography. When we look at all these techniques, we found that Steganography gives more security comparatively other methods. As well as digital communication technology has changed security features also required some variations. Information security attracted many researchers and has become the widely scoped area of research in wireless and mobile communication. The field of Steganography is very vast, but researchers have been motivated toward mobile steganography because of the intensive use of mobile phones as well as the exchange of information among the users. In the same context, “Short Messaging System (SMS) was introduced with GSM mobile phones and became too much popular among users” [2]. After some time, the multimedia message was introduced and gained more popularity due to its advanced features. Later, smartphones have come to light with many advanced features for communication. It is a small handy portable device that the user can carry with him anywhere. Thus, users can use these devices in various ways like photo capturing, sharing of information in images, audios videos and calling, etc. To stop unauthorized access and attacks, we must have to use systems with some data security techniques. We have described few data security techniques earlier in which one of the trendiest techniques is steganography.

II. Steganography

We start with the security of information that so many techniques are present. Fig. 1 depicts the different disciplines of information hiding. Steganography alludes to the study of "imperceptible" correspondence. In contrast to cryptography, where the objective is to make safe correspondences from a user, steganographic strategies endeavor to hide the very nearness of the message itself from an onlooker [4]. Steganography is the craftsmanship and study of imparting so that the nearness of a message can't be distinguished [5].

Steganography is the science that includes imparting mystery information in a suitable sight and sound bearer, e.g., Image, sound, and video. It goes under the presumption that if the element is noticeable, the purpose of assault is obvious, therefore the objective here is consistently to disguise the very presence of the installed information [9]. The word steganography is of Greek cause and signifies disguised composition from the Greek words steganos (στεγανός) signifying secured or ensured, and graphei (γράφη) signifying composing. The principal recorded utilization of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography masked as a book on enchantment. By and large, messages will give off an impression of being something different: pictures, articles, shopping records, or some other spread content, and, traditionally, the concealed message might be in undetectable ink between the obvious lines of a private letter [14]. Steganography implies concealing the presence of data in such a way along these lines that nobody can recognize. Three procedures of data security are fundamentally the same Cryptography, watermarking, and steganography. Pictures are used as the bearer to perform steganography. A mystery message is implanted in the transporter picture so that nobody can recognize that mystery message. Ancient steganography worries about the ways of inserting the mystery message in a spread picture. The implanting needs key without which an outsider cannot identify or evacuated the original message. The cover picture with the implanted message is called Stego Image.

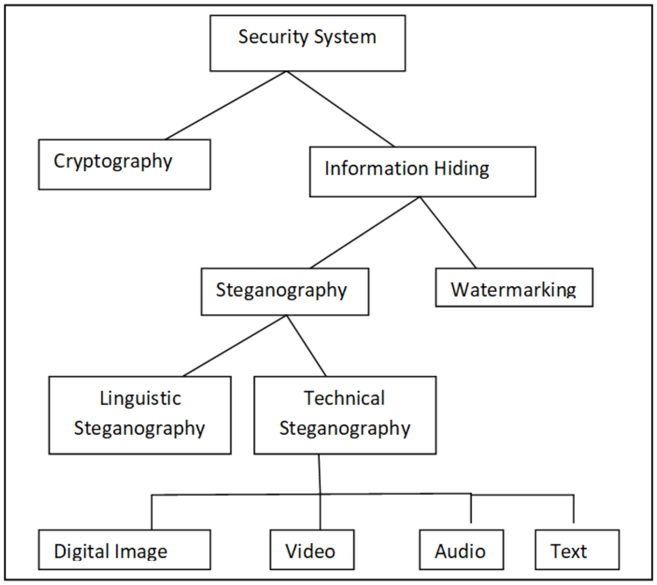


Fig. 1. Types of Security System.

A. Working of Steganography

A steganography algorithm shows a combination of a mystery message-which needs to cover up, picture – which contains the implanted message. The general working of steganography is to get the message to stow away, get the picture wherein information to cover up, Apply the suitable algorithm which produces the stego picture. This Stego picture sends to the beneficiary, receiver interprets the stego picture and gets the first message.

With the help of Fig. 2 general idea of steganography can be understood.

The message is the information that the correspondent needs to keep secret. It may be a plain content, figure text, another picture, or something that can be implanted in a bitstream, for example, a patent mark, an incognito correspondence, or a sequential digit. Key is a particular word, which guarantees that the beneficiary who realizes the relating disentangling key will have the option to remove the message from a Stego picture. The spread picture is likewise called a transporter. The generated picture with the secretly inserted message is known as the stego message. Recouping data from a Stego image requires the stego picture itself and a relating deciphering input if the input is used throughout the encoding procedure.

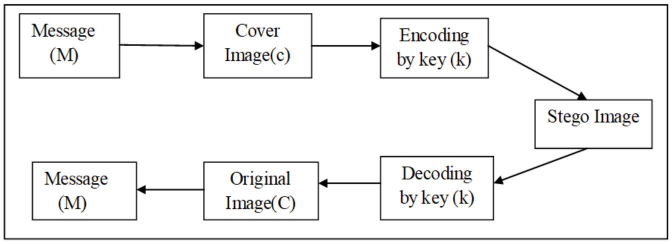


Fig. 2. Representation of Steganography.

III. Cryptography

Cryptography is the preparation and examination of disguising information. It consolidates the request for number juggling, programming building, and electrical structuring. Cryptography is encryption, which is the route toward changing over standard information into muddle information. Deciphering is the opposite system of getting authentic information from confounded information.

A. Working of Cryptography

A cryptographic estimation works in blend in with a keyword, number, or articulation—to encode the plain text. The proportional plain text scrambles to different text with different keys. The security of encoded data depends on two things: the nature of the cryptographic estimation and the secret key. A cryptographic algorithm, in addition to every potential key and all the conventions that make it work, involves a cryptosystem. With the help of Fig. 3, the general idea can be comprehended.

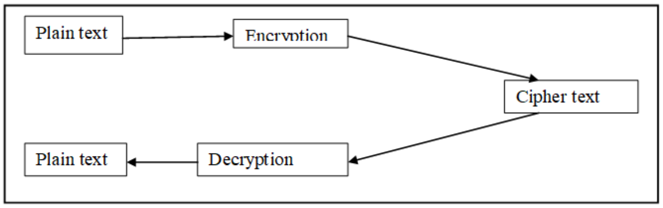


Fig. 3. Cryptography Concept.

IV. Literature Review

Most of the work has been done in the field of steganography. Mainly steganography has been done on bit map pictures, gif pictures, and grayscale pictures.

The most widely recognized and easiest steganographic technique is the least significant bit inclusion strategy is presented earlier. The least Significant Bit Substitution strategies are called due to how the message information m is inserted inside a spread picture c. In software engineering, the word Least Significant Bit (LSB) alludes toward the littlest (right-most) piece of a parallel succession. The organization of binary is with the end goal that every number may just be either a 0 or a 1, frequently idea of as on separately. Beginning from the right, the worth (if on) signifies a 1. The incentive to one side (if on) means a 2, etc. wherever the qualities are twofold every time [1]. Afterward new encoding strategy utilizes a matrix. The best appropriate procedure for jpeg steganography is considered F5 algorithm [2]. The first recorded use of steganography found from 440 BC back when Herodotus informed to Greece about the forthcoming attack by writing a message on the wooden and covered it by wax. Another example of ancient steganography is Histiaeus who shaved the head of his slave and tattooed the message on it after hair grown message was hidden [3]. In this author has provided the review of steganography techniques and steganalysis technique [4]. According to this paper, a secure stego system is proposed using the stego text distribution close to the cover text distribution. Here observer no need to know about the secret key. The embedding function depends on the cover text distribution [5]. This paper presented and discussed the possibility for using steganography in MMS and also suggested SMILE Steganography. Here presented algorithms and evaluation are on theoretical basis only [6].

As well as mobile phones became popular, so MMS techniques were used for communication. So, there was also some research in such area which shows the calculation for hiding information in MMS utilizing Portable Network Graphic picture also shows the novel strategy for steganography utilizing both content and pictures [7]. Steganography technique used in a game known as the Sudoku puzzle. It shows that how we can hide data in the Sudoku puzzle for secure information transfer [8]. In this paper different analysis of existing steganography has been done. Here are also given some differences between steganography and watermarking. Some questions may also arise such that is this technique is useful or not? [9]. Here we find how we can use steganography in MMS for Smartphones. Two-level of security has provided using image and text both [10]. Here author suggested Elliptic Curve Cryptography method for MMS security purpose [11]. This paper gives a comparative study of different mobile environments and their development technology. Also, introduce security issues for android OS [12]. In this paper authors provided steganography for JPEG image over the mobile phone. Here algorithm is implemented through the combination of text, image, and encryption [13]. This paper gives idea of hiding the text message inside one small image using LSB and then hided that image in larger image using DWT algorithm. It is implemented on gray images not on color images [14]. In this paper author implemented steganography method on android environment using LSB method and also used TEA algorithm for cryptography also for reducing the size of message LZW compression method is used [15]. Multi-Level steganography with dissemination in painting and YASS Algorithm on the external level and One-Time stuffing of the mystery note with key picture and YASS on internal level used for steganography [16]. In another paper author described about a model called Ste-Chy as an evidence of idea of the blend of the strategies. This methodology helps the client as far as the trading of secret information by online offer in Android base media. In support of the classified confirmation reason, the secret message is concealed along with the objective picture. At an adequate level image is created by this work using nature of original and stego pictures [17]. In [18] authors were used emoticons or lingoes to hide the information. He has proposed his idea for embedding data in emoticons or using lingoes in SMS than the recipient can extract the hidden information. In [19] we find the information regarding different steganographic techniques and gives performance metrics for mobile image steganography. In [20], creators have built up an android application through which we can shroud information behind the picture, and we can share an apk document through WhatsApp. This application is created by utilizing steganography and the LZMA firmness strategy. In this research authors have given idea of video watermarking using steganography. For steganography they have used DCT method. Here water mark is embedded inside the quantized coefficients [21]. It gives improvement in multiphase encryption by encrypt the data with different encryption algorithms. Here proposed algorithm itself append the information along with secret text on the other hand in multiphase sender provide the specific order to receiver for decrypting the message [22]. In this work creators suggested Image steganography using k means clustering and AES encryption together. Messages are hided in object area which form as cluster with that encryption has also used for improvement [23]. Benefit of this application is it gives twofold security by utilizing hiding and firmness strategy. For jpeg image, a steganography technique is proposed. A part of data may be lost after the quantization of frequency values in the JPEG compression procedure, in the proposed method, the embedded message is added to the image after the discretization stage. The method utilizes two adjacent pixels in the steganography process [24]. The authors suggested cryptography and Steganography method for smart phones. Here they have used RSA algorithm for encryption and LSB insertion method for information hiding [25]. Message is sliced in parts and hided in multiple images. LSB technique is used for each image and image contain some header information so that at the receiver side any specific order is not required [26]. This paper gives idea of different techniques for jpeg steganography. It summarizes various algorithms and techniques used in the past and in present. This paper also analysis's these algorithms based on the basic parameters of image steganography: Unidentifiable, robustness and hiding capacity [27]. Here author proposes a JPEG steganography algorithm to provide strength to the Stego image using DCT coefficient and maintain an even coefficient distribution based on the JPEG characteristic [28]. In this paper author has suggested LSB embedding method using BMP and PNG images. He has hided secret message in pixel values and modified values have shown in new generated images [29]. "This paper introduced the concept of steganography using bit selection of cover image. Basically, here also LSB Technique is used for hiding the secret message. Message can be in any format text or image. Here gray scale image has been taken as example to perform this operation. Secret message image must be smaller then cover image [30].This paper suggested the modification in F5 algorithm of data hiding. It is based on idea of modified matrix embedding (MME). In proposed method all nonzero AC coefficients collected in single array and divides array into small coefficient blocks, then find the coefficient with least distortion to embed message [31].

The rise of mobile phones has led to new demands of android operating systems and applications to run on it. Nowadays image steganography is a very wide area for research work. The field steganography is very vast but, in that field, and the present requirement mobile steganography work motivates the researchers to introduce some new and innovative ideas. Steganography poses a lot of interesting research problems and there are so many techniques to implement it and require some further improvement. There is still not too much work that has been done on JPEG steganography over cell phones.

V. Motivation

There is too much research that has been done on image security over the different kinds of image formats BMP, GIF, and PNG. Several compression methods are available that applied to the image having the formats BMP, GIF, and PNG is comparatively less effective than the JPEG image. Even the

JPEG compression steganography method becomes difficult though some algorithms show JPEG Steganography. But they provide a single-level or two-level security. Most of the techniques are computer system based but not for mobile phones. Now day's everyone has a mobile phone became so handy. Chatting is one popular application of mobile through which one can share different kinds of data such as pictures, audio, and videos among users. When we consider information security over mobile phones, steganography is the best security procedure because most of the correspondence with the assistance of sharing pictures. Although steganography has been done in all types of image format still this technique is an interesting research area for mobile application. The motivation for this work is that steganography is the way to provide secure communication. Its main goal is to hide information so that no one can detect it and provide information securely to the sender. Hackers or attackers cannot identify the hidden message in any way. In this carrier, the image keeps a secret message and looks like an original image so that intruder cannot pay attention to it. Most security agencies are using this technology for secure communication. In the present scenario, the mobile phone has become a popular device for communication due to which information flows freely, so information security becomes a primary concern. Hence this motivated mobile application development.

VI. Proposed Method

Earlier work is carried out using text steganography and image steganography and for this purpose PNG (Portable Network Graphic) image was used [7].

In this work, we are using JPEG images for steganography. We will encrypt an original text message two times later split it into two halves to hide the first half in the image and the second half in the cover message.

Steps for procedure:

Input: An Image (Cover Image), Text message (Plain Text), Text message to hide

Output: Stego Image with hidden Text, One text file

1) Write Text to hide.

2) Take original image known as cover image.

3) Write Short text message which is known as plain text.

4) Encrypt the text which to be hidden using DES algorithm.

5) Re-encrypt the received encrypted data using the DES algorithm again to produce ciphertext.

6) Split the cipher text in two halves.

7) Hide the first half cipher text in Cover image using matrix encoding algorithm.

8) Hide the second half cipher text in cover message using markove chain method.

9) Generate stego image and one text file.

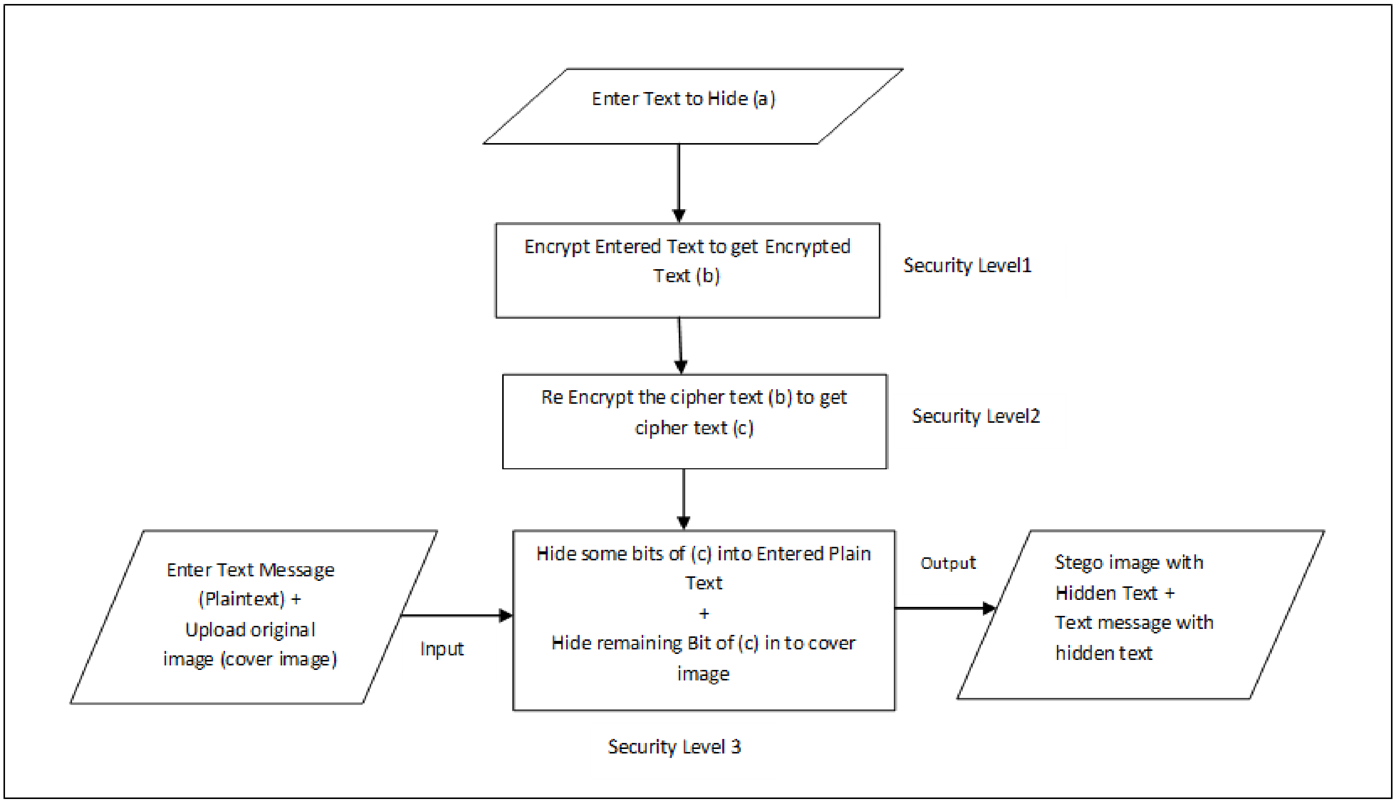

Enter Text to Hide (a)
Encrypt Entered Text to get Encrypted Text (b)
Security Level1
Re Encrypt the cipher text (b) to get cipher text (c)
Security Level2
Enter Text Message (Plaintext) + Upload original image (cover image)
Input
Hide some bits of (c) into Entered Plain Text + Hide remaining Bit of (c) in to cover image
Output
Stego image with Hidden Text + Text message with hidden text
Security Level 3

Fig. 4. Workflow Diagram.

For receiver side follow the procedure in reverse order but there we provide Stego image, Cover message and generated text file as input to extract original message Fig. 4 shows the basic idea of workflow.

Algorithm

S1: Select the image on which we have to perform operation called original image.

S2: Enter the message which must be hidden.

S3: Enter Cover Message which is used for text steganography.

S4: Apply DES Algorithm on message enter in step2 to get encrypted text.

S5: Again, apply DES algorithm on received encrypted text from previous step to get final cipher text

S6: Divide the final cipher text in two halves

S7: Take one half of cipher text and Image loaded in Step1 and Apply F5 algorithm to hide the text in image

S8: Take the other half of cipher text and Cover message (S2) apply Markov chain method to hide cipher text in cover message

VII. Implementation

To encrypt the text which has to hide, "DES Algorithm" has been used in this paper. We encrypted the text first by DES algorithm through which we received Encrypted Text and Further that encrypted text is encrypted again through the same DES Algorithm to get final ciphertext. After receiving this ciphertext, we have split the ciphertext in two half one portion to hide in the image and the other portion to hide in text. We have used the F5 algorithm to hide the text inside the image. It is most commonly used an algorithm based on matrix encoding.

We do quantization of coefficient and then we embed the message using bit position and performing XOR operation. We can understand it through an example.

We want to embed Two bits p1, p2 in three-bit places q1, q2, q3 changing one place at most.

There may be four condition arises. If we find p1 is equal to XOR operation between q1 and q3, and p2 is equal to XOR operation between q2 and q3 then we don't change in bits.

If we find p1 is not equal to the XOR operation between q1 and q3, and p2 is equal to the XOR operation between q2 and q3 then we change bit q1.If we find p1 is equal of XOR operation between q1 and q3, and p2 is not equal of XOR operation between q2 and q3 then we change in bits q2 bit.

If we find p1 is not equal of XOR operation between q1 and q3, and p2 is not equal of XOR operation between q2 and q3 then we change in bit q3. In all these conditions we do not change more than one bit.

Text hiding within text:

Hide text in text with the help of cover messages using a Markov Chain method. This generates an encryption vector based on the relationship between the cumulative character score of the cover message and each character of an input string. Decrypt messages by reversing the encryption on the encryption vector and retrieving the original message based on the cumulative character score and the relationship between the cover message and the input string.

Generating an Encryption Vector:

Take the sum of all the ascii character codes of each character in the cover message:

Example: hello,

h = 104, e = 101, l = 108, l = 108, o = 111

Sum hello = 104 + 101 + 108 + 108 + 111 = 532, this forms the cumulative character score S. Append the difference of S and the ascii character value of the input string to an Array List to form the encryption vector

S = 532

Input = "dog", d = 100, o = 111, g = 103

Evector = {532 – 100, 532 – 111, 532 - 103} = {432, 421, 429}

To hide the text encryption vector Evector, use AES – 256 Encryption Algorithm to encrypt the Array List for message. For retrieving the information at receiver side, the received Message and its Evector are first decrypted by initializing a Java Cipher object in decryption mode using the secret key yielding a decryption vector Dvector. Then it follows reverse process to get original message. Here Fig. 5 represent the GUI of developed app.

Fig. 6 Show the encoding view though which user can enter original and cover message.

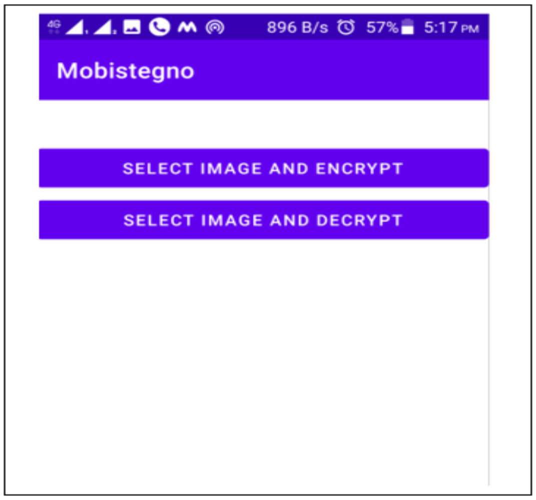
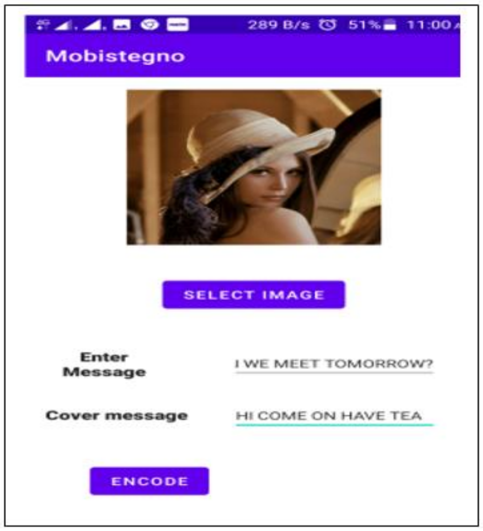


Fig. 5. App Start View.

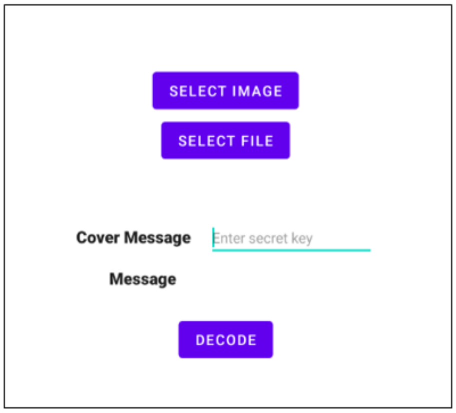


Enter Message: I WE MEET TOMORROW?

Cover message: HI COME ON HAVE TEA

Fig. 6. Encoding View.

Fig. 7 depict the decode view of app in which user can enter the cover message to get back original message.

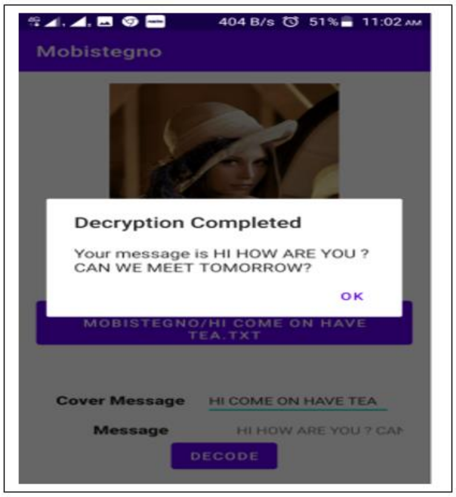


Cover Message: Enter secret key

Message

Fig. 7. Decode View.

Here the Fig. 8 represent the result view where user get original message.



Decryption Completed

Your message is HI HOW ARE YOU ? CAN WE MEET TOMORROW?

Cover Message: HI COME ON HAVE TEA

Message: HI HOW ARE YOU ? CAN

Fig. 8. Result View.

VIII. Result and Discussion

When we embed the data in the image it increases in the Mean Square Error (MSE). This automatically reduces the Peak Signal to Noise Ratio (PSNR) and vice versa. The PSNR is to be measured in decibels (dB). Usually, PSNR of more than 35db is considered good quality, so our results have good values. The lesser the MSE value higher will be the PSNR values. Equation 1 shows the formula for calculating PSNR.

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \qquad (1)$$

$$= 20.log_{10}(MAX_I) - 10.log_{10}(MSE)$$

Formula for calculating mean square error is given by equation 2.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (2)$$

It shows the changes between the original image and the stego image. Here m and n show height and width of the image.

We have used different images to embed the data inside. Here one message is conveyed, and text is hidden inside the image. Also, some part of the text is hidden in cover message. Here we have used three-level security for data hiding on the android environment. Table I shows the comparisons of features. Table II shows the PSNR values for different images hiding the different data. Original images contain the secret data which produces stego images. The PSNR value gives the peak signal-to-noise ratio.

Cover message for image 1: hi come on have tea.

Message to hide: hi how are you? Can we meet tomorrow?

Cover message for image2: good morning dear friend

Message to hide: dear ajay thanks for making life fun and being my friend you are most amazing person I know.

Cover message for image 3: we need urgent meeting

Message to hide: This is very important message. There is chance of terrorist attack we need army

We have implemented this on Android SDK and tested on Lenovo k6 Note also run-on Android emulator. We have calculated the PSNR and MSE values on NetBeans IDE.

TABLE I. Comparison of Algorithms

Features	**F5Algorithm**	**Previous Algorithm**	**Proposed Algorithm**
Color	Yes	Yes	Yes
Format	JPG	PNG, GIF	JPG
Security	Yes	Yes	Yes
Micro	No	Yes	Yes
Android Device	Need Modification	No	Yes

TABLE II. COMPARISON OF ALGORITHMS

Original Image	Image after Steganography	MSE Value	PSNR Value
Original Image1,JPG	Stego Image1.JPG	0.15%	46.27
Original image2.JPG	Stego Image2.JPG	0.69%	39.69
Original Image3.JPG	Stego Image3.JPG	0.39	42.18

Fig. 9. Original Image 1.

Fig. 9, Fig. 11 and Fig. 13 show the original images through which the secret message migrated.

Fig. 10. Stego Image 1.

Fig. 10, Fig. 12, and Fig. 14 represent the stego images that contains the hidden message. For retrieving an original text, these stego images are used.

Fig. 11. Original Image 2.

Fig. 12. Stego Image 2.

Fig. 13. Original Image 3.

Fig. 14. Stego Image 3.

IX. CONCLUSION

As we know that technologies have been improving in the field of communication, its result is that many microdevices have also arrived in the market. The most commonly and widely used device is the android smartphone. In such environments, the concern of security may arise that how can we keep protected our data and information. For this purpose, many researchers have used either cryptography or Steganography techniques. Some of them also tried a combination of both. When we see the previous work we found that very little work has been done over JPEG image format in the android environment and whatever the work has done they have to provide only one level or two-level security. Here we have given a method for enhancing the security by using cryptography and Steganography at three-level security over the android environment. Here hiding information in two different parts that are image and text makes it more robust to attack. We have encrypted the message two times with the DES Encryption algorithm and then divide that encrypted message into two halves so that one part is hidden in the image using the F5 algorithm and another part is hidden in the cover message using the Markov chain method for text Steganography. In this manner, two times encryption and further hiding in text and image make this system the best application to ensure data security. Till now F5 algorithm implementation is not available for android application so it is very secure application for image steganography over mobile phone. It is extensively using DES algorithm with f5, so it takes some time in processing. In comparison of other this method has advantage of security at three level which has not implemented till now on android phone using F5 algorithm for JPEG images. The limitation of this application is that it is tested on the upper than android 6 version not supported on the lower version and gives the best result for short messages, not for long payload.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu "Techniques for data hiding." IBM systems journal 35, no. 3.4 (1996): 313-336.

[2] A. Westfeld,"F5—a steganographic algorithm. Information hiding." In 4th International Workshop, LNC8, vol. 2137, pp. 289-302. 2001.

[3] N. Provos, P. Honeyman.," Detecting steganographic content on the internet". Center for Information Technology Integration, 2001.

[4] R. Chandramouli, M. Kharrazi, and N. Memon. "Image steganography and steganalysis: Concepts and practice." In International Workshop on Digital Watermarking, pp. 35-49. Springer, Berlin, Heidelberg, 2003.

[5] C. Cachin, "An information-theoretic model for steganography information and computation, 192(1), 41-56,2004.

[6] K. Papapanagiotou, E. Kellinis, GF. Marias, and Panagiotis Georgiadis. "Alternatives for multimedia messaging system steganography." In International Conference on Computational and Information Science, pp. 589-596. Springer, Berlin, Heidelberg, 2005.

[7] M. Shirali-Shahreza,"Steganography in MMS. Multitopic Conference, INMIC 2007." In IEEE International Conference. 2007.

[8] M.H. Shirali-Shahreza, M. Shirali Shahreza,"Steganography in SMS by Sudoku puzzle." In 2008 IEEE/ACS International Conference on Computer Systems and Applications, pp. 844-847. IEEE, 2008.

[9] A. Cheddad, J. Condell, K. Curran, and P.Mc. Kevitt. "Digital image steganography: Survey and analysis of current methods." Signal processing 90, no. 3 (2010): 727-752.

[10] D.D. Dhanashri, S.P. Babaso, and H. P. Shubhangi. "Mms steganography for smartphone devices." In 2010 2nd International Conference on Computer Engineering and Technology, vol. 4, pp. V4-513. IEEE, 2010.

[11] B.N. Jagdale. K. Bedi, and S. Desai. "Securing MMS with high performance elliptic curve cryptography." International journal of computer applications 8, no. 7 (2010): 17-20.

[12] J.P. Laverty, D.F. Wood, F.G. Kohun, and J. Turchek. "Comparative analysis of mobile application development and security models." Issues in Information Systems 12, no. 1 (2011): 301-312.

[13] Y.K. Jain, R. Kumar, and P. Agarwal. "Securing data using JPEG image over mobile phone." Global Journal of Computer Science and Technology (2011).

[14] I. Badescu, C. Dumitrescu. "Steganography in image using discrete wavelet transformation." In Proc. WSEAS Conf. on Advances in Mathematical Models and Production Systems in Engineering, Brasov, Romania, pp. 69-72. 2014.

[15] M.S.A. Putra, G. Budiman, and L. Novamizanti. "Implementation of Steganography using LSB with Encrypted and Compressed Text using TEA-LZW on Android." In 2014 International Conference on Computer, Control, Informatics, and Its Applications (IC3INA), pp. 93-98. IEEE, 2014.

[16] C.V. Amruth, P. P. Amrita. "Multi-level steganography for smart phones." In 2014 First International Conference on Networks & Soft Computing (ICNSC2014), pp. 81-84. IEEE, 2014.

[17] C. Danuputri, T. Mantoro, and M. Hardjianto. "Data Security Using LSB Steganography and Vigenere Chiper in an Android Environment." In 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), pp. 22-27. IEEE, 2015.

[18] V. Iranmanesh, H.J. Wei, S.L. Dao-Ming, and O.A. Arigbabu. "On using emoticons and lingoes for hiding data in SMS." In 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET), pp. 103-107. IEEE, 2015.

[19] D. Bucerzan, C. Raţiu. "Testing methods for the efficiency of modern steganography solutions for mobile platforms." In 2016 6th International Conference on Computers Communications and Control (ICCCC), pp. 30-36. IEEE, 2016.

[20] S.A. Dhanawe, S.V. Doshi. "Hiding file on Android Mobile and Sending APK file through whats app using Steganography and Compression techniques." In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 106-110. IEEE, 2016.

[21] M.G. Busiri, R. Munir. "Mobile Application of Video Watermarking Using Discrete Cosine Transform on Android Platform." In 2017 5th International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), pp. 207-211. IEEE, 2017.

[22] H. Kaur, H.P.S. Gill, and D. Sarmah. "Multiphase and Multiple Encryption." IEEE Punecon, pp. 1-8. IEEE 2018.

[23] A.A. Lubis, R. Purba, and I.A. Pardosi."Combination of Steganography with K Means Clustering and 256 AES Cryptography for Secret Message." In 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1-4. IEEE, 2019.

[24] A. Darbani, M.M. AlyanNezhadi, and M. Forghani. "A new steganography method for embedding message in JPEG images." In 2019 5th conference on knowledge-based engineering and innovation (KBEI), pp. 617-621. IEEE, 2019.

[25] R. Kofi Kyei, J.K. Panford, and J.B. Hayfron-Acquah. "Enhancing data security in android smartphones using image steganography, RSA encryption with LSB insertion", 2019.

[26] A.G. Benedict, "Improved file security system using multiple image steganography." In 2019 International Conference on Data Science and Communication (IconDSC), pp. 1-5. IEEE, 2019.

[27] D. Watni, S. Chawla. "A comparative evaluation of jpeg steganography." In 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 36-40. IEEE, 2019.

[28] J.T. Kim, S. Kim, and K. Kim. "A Study on Improved JPEG Steganography Algorithm to Prevent Steganalysis." In 2019 International Conference on Information and Communication Technology Convergence (ICTC), pp. 960-963. IEEE, 2019.

[29] J.A.R. Kazi, G.N. Kiratkar, S. S. Ghogale, and A.R. Kazi. "A novel approach to Steganography using pixel-based algorithm in image hiding." In 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6. IEEE, 2020.

[30] A. Thakur, G. S. Gill, and S. Saxena. "Analysis of Image Steganography Performance Check Using Bit Selection." In 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 1-5. IEEE, 2020.

[31] M. Amiruzzaman, R.M.Nor. "Hide Secret Information in Blocks: Minimum Distortion Embedding." In 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 107-112. IEEE, 2020.