Multimedia Multilevel Security by Integrating Steganography and Cryptography Techniques

E G Satish[*1], N. Sreenivasa[2], E. Naresh[3], P. Ramesh Naidu[4], Ramachandra A C[5]

[1,2,4,5] Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Yelahanka, Bangalore-560064
[3]Department of Information Technology, Manipal Institute of Technology, Bengaluru, Manipal Academy of Higher Education, Yelahanka, Bangalore-560064

satish.eg@nmit.ac.in, sreenivasa.n@nmit.ac.in , naresh.e@manipal.edu , ramesh.naidu@nmit.ac.in , ramachandra.ac@nmit.ac.in

Abstract. Multimedia-based Steganography is famous for its security purpose, These steganography techniques were used by our ancestors and it is still carried out now with better and vast technology. The aim is to provide better security in an effective and secure manner where the original data is covered and hidden by some of the media covers like video, audio, image, text, etc. so that only the sender who sends it and the receiver who receives it can only see the secret data inside it. In this project, we are combining all the steganography types and giving the user the advantage of selecting his/her own choice of multimedia cover to hide the real content. The options of the different algorithms will be provided so that the users who are comfortable with that algorithm have the privilege to select it and the file will be processed with that algorithm. This steganography technique is used by the government to send information that supports national security, The company uses it for digital copyrighted media, and military services also use this technology to send it to the army who are on a mission. We aim to provide the same with more security and a rich user experience. In this survey, a variety of methods is used to provide the same facility and recent research in the field.

***Keywords*—**Steganography, Cryptography, LSB, PSNR, steno image, AES.

1 INTRODUCTION

Steganography has been obtained from the Greek words “Stego” which means “Covered” and “Graphia” which means “writing”. This term was first introduced in 440 B.C in Greece but modern and advanced steganography was first coined in 1985 when people’s computers begin applied to classical steganography. Special "inks" were used as stenographic tools during the Second World War[1][2]. Data concealment-supported text has become the most

* satish.eg@nmit.ac.in

popular and most mentioned side of steganography in recent years. The aim of Stenographic communication back and now, in the modern application, is the same i.e., to hide secret data.

2 RELATED WORK

In today's Society, Communication is the basic desire of the developing space. Everybody needs the privacy and security of their personal knowledge.

Though we often share and transfer knowledge across secure channel like phone or telephone and the internet, these medium doesn't seem to be entirely secure [3]. So as to share the knowledge having privacy two techniques area unit i.e., Cryptography and Steganography. In cryptography, the communication is converted to an encrypted one by the use of an encryption key that is only known to the sender and the recipient. However, posting an encrypted message can merely raise an attacker's suspicions; leading to the message to violently intercepts attack or read. To overcome these steganography techniques are developed. Steganography is a communication method that provides art and science to operate in a way such that no one can detect its use in communication. Thus, it hides data in order to protect the data and hides the presence of its detection. In steganography, "it hides information in any content like image, audio, and video is referred as a ―Embedding". For increasing the confidentiality of the act of knowledge each of the techniques could also be combined. Steganography could hide information in computer files [4][5]. Electronic communications might involve Steganographic secret writing in digital steganography inside a tcp protocol, as in a document, image file, software, or protocol. Media like audio and video are ideal for steganographic transmission because of their large size. In steganography, LSB (Least significant bit), PVD (Pixel value difference), Pixel indicator, Discrete Cosine Transform, and Discrete wavelet transform methodologies are used whereas in cryptography ECC (Elliptic Curve Cryptography) and RSA(Rivest–Shamir–Adleman) methodologies are used. The Methodology ought to have imperceptibility, robustness, capacity, secrecy, and accuracy.

Nowadays Steganography is used in different fields to secure data from hacking and to protect sensitive data confidential. Some of the used areas are:

- Communication and data are secure and confidential.
- Used in E-Commerce
- Used for media Database Systems
- Used in Digital Watermarking
- Data Alteration is protected
- Digital Content Distribution Control system is accessed

LSB-related image steganography is done on the basis of attributes like resolution and file type in [6]. This paper discussed the use of RGB images which enhances the image quality and also increased the hiding capacity.

In Rutvik Dumre [6] has improved the limitation of the old LSB method. However, the author[9] was not able to implement this method for black and white images. Similarly, in [7] author has used the RGB planes to embed the data changing the RGB bits of an image. In [8][10] the author has discussed the encoding and decoding algorithm of PVD.

DCT converts the data from spatial to frequency form [11]. DCT provides a high PSNR value which indicates that the original image and stego-image have high similarity. We know that the DCT function is applied only on grayscale images. So, if the image is in the form of RGB then we first convert it into the grayscale form [12] and then apply the DCT function to it. In [13] using the AES algorithm, the secret message is encrypted using a key-generated MD5 hash function. In [14] two types of hashing algorithms can be used i.e., SHA1 and MD5. In [15] the message is encrypted by using the AES algorithm. In [17] based on the image information using the SHA algorithm a digital watermark is created. Based on the research [16] ECC is much better in terms of performance and has a shorter key length than the RSA encryption technique [18].

A. Types of Steganography

Confidential data hiding technique has been classified in different forms on the basis of the uses of cover image as well as the type of data that is to be hidden.
Image Steganography**:** The process of hiding data under a cover image and changing the pixel value of the images is shown in Figure 1.

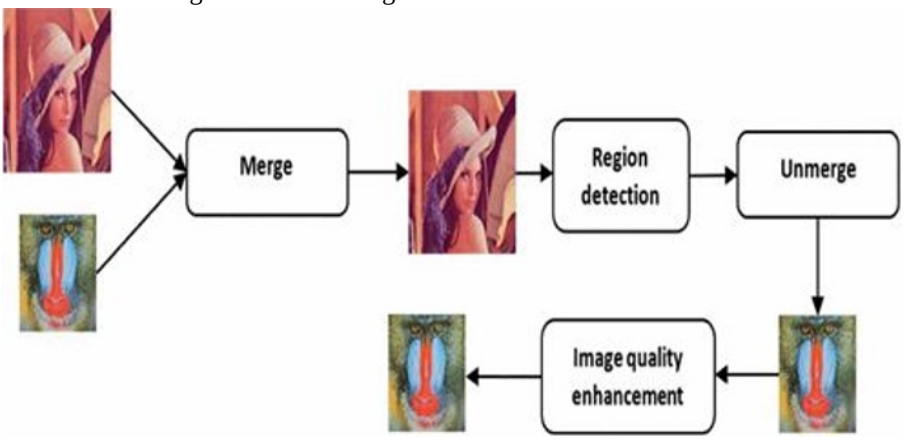

Figure 1: Image Steganography

Network Steganography: The unused header bits of TCP/IP fields are used here for the steganography process and the network protocol is used as cover objects as shown in Figure 2

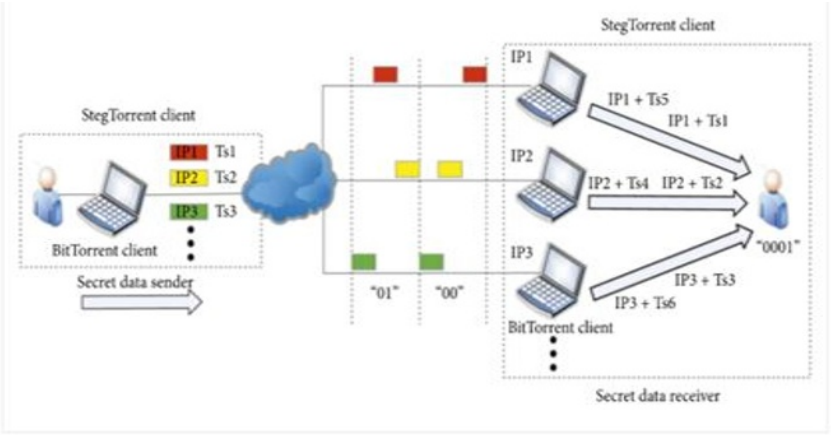

Figure 2: Network Steganography

- Video Steganography**:** Information is hidden under a video file. DCT alter values are used to hide the information on a few of the images of the video file is as shown in Figure 3.

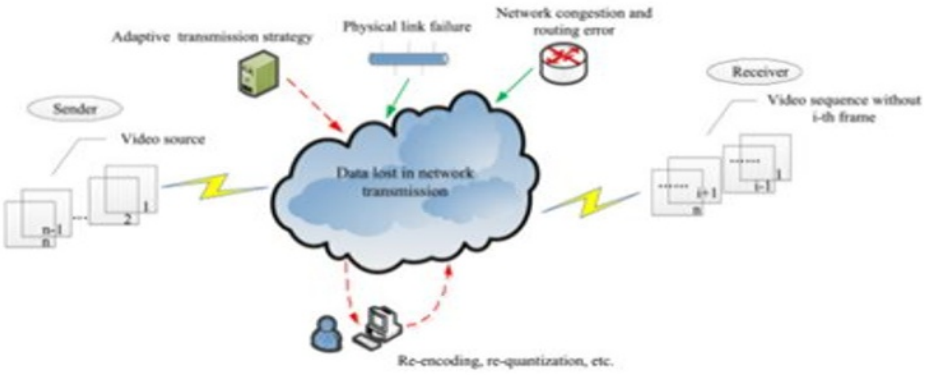

Figure 3: Video Steganography

- Audio Steganography**:** Due to the VOIP facility digital audio formats like WAVE, MIDI, etc are used as a carrier for information hiding is as shown the Figure 4.

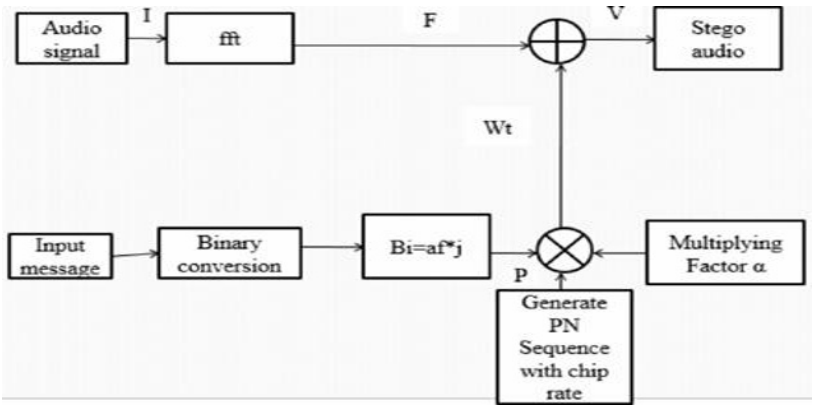

Figure 4: Audio Steganography

- Text Steganography**:** Text steganography (Figure 5) is achieved by utilizing white spaces, and tabs rearranging words. It is the process of concealing one text message into another text message as a cover message[4].

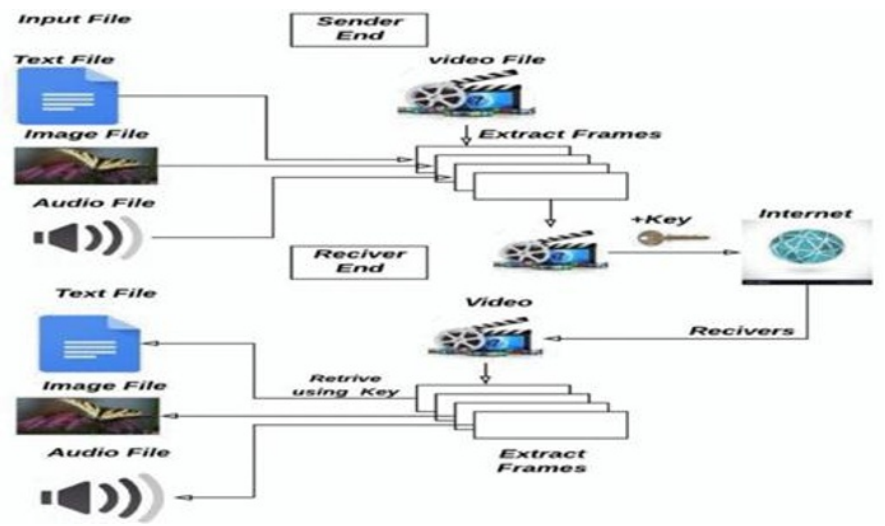

Figure 5: Text Steganography

I. Study of Tools/Technology

A. LSB Technique

One of the most used methods for image steganography is LSB. It is all about changing the last bit of the image pixel. The basic approach of the LSB technique is to embed the data in the LSB of all the pixels of the cover image and the image produced after embedding the data is known as stegoimage as shown the Figure 6. As we know that each pixel of an RGB image consists of 24 bits and each color is made up of 8 bits. Each color has 256 intensity levels. Hence changing the least significant bit of the

image will result in a small color difference that is not recognized by the human eye.

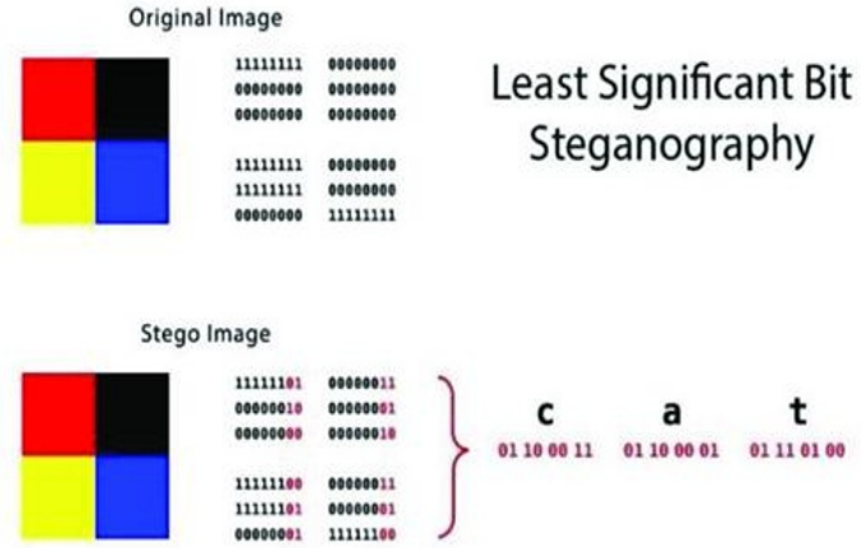

Figure 6: LSB Technique

B. PVD Technique

PVD stands for pixel value differencing. In this method, the cover image is divided into two-pixel blocks which are non-overlapping. The new and old value of pixel can be used to calculate the difference and hence the pixel value can be modified. The pixel values excluding the first and second row are scanned one by one in raster scan fashion in decoding part of PVD. They are the transferred in to characters after converting the binary forms and these characters joins together to create the secret data which is hidden inside the image.

C. Discrete Cosine Transform (DCT)

First, the image is broken into 8X8 blocks which get transferred to 64 DCT coefficients using 2D DCT. And for the decoding process, the inverse of 2D DCT is performed which in return generates the spatial form. When DCT performance is analyzed on the basis of PSNR (Peak Signal to Noise Ratio) and its payload capacity, DCT provides a high PSNR value which indicates that the real image and stego-image have a high similarity[7].

D. AES (Advanced Encryption Standard)

AES means Advanced Encryption Standard. It uses symmetric block ciphers which encrypts and decrypts the message. In order to encrypt the word in 128 bits, it uses different keys 128 bit, 196-bit,256 bit. There are 4 distinct types of stages used, one of permutation and three of substitution: -

- Substitute bytes: This method utilizes an S-box to perform a byte-by-byte substitution of the block
- Shift Rows: means a simple permutation

• Columns Mix: A substitution that uses arithmetic over the Galois field.
• Add Round Key: This method uses a simple bitwise XOR of the current block with a portion of the expanded key.

E. SHA (Secure Hash Algorithm)

SHA means a Secure Hash Algorithm (Figure 7) which is one of the cryptographic hash functions which takes an input and gives the output of a 160-bit (20-byte) hash value known as a message digest. This hash value is usually referred to as a hexadecimal number which is long as 40 digits. It is developed by the United States National Security Agency.

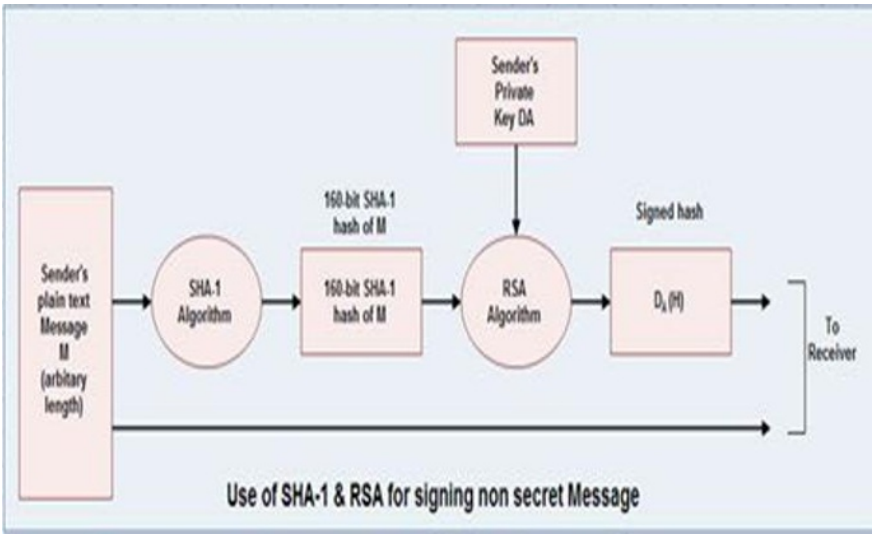

Figure 7: Secure Hash Algorithm

F. ECC (Elliptic Curve Cryptography)

The cryptographic technique (Figure 8) uses the ECC protocol. ECC is much better in terms of performance and has a shorter key length than the RSA encryption technique. ECC is a public key system that uses an elliptic curve having equation y = (x^3 + cx +d) mod q, where (4c^3 + 27d^2) mod q≠0. Here changing the value means creating a new ECC curve.

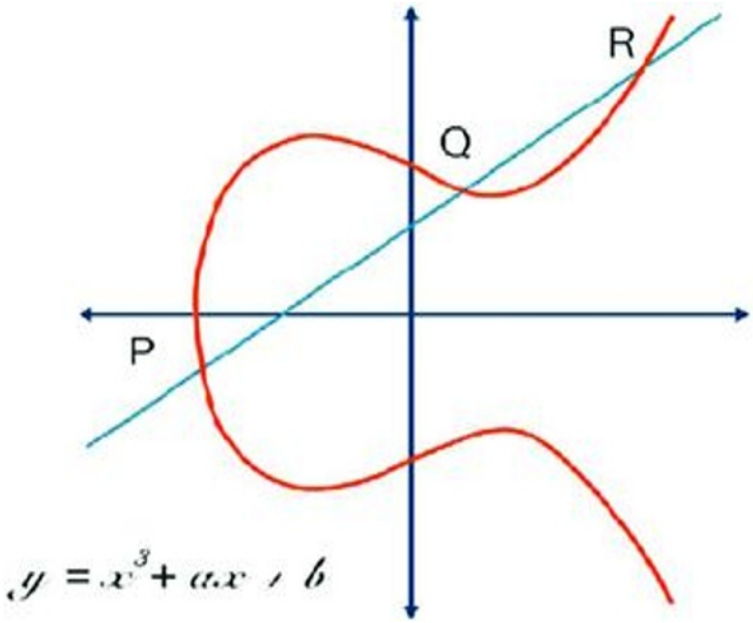

Figure 8: Elliptic Curve Cryptography

Combining Steganography with Cryptography provides a guarantee of security to the digital media that get transferred through an online source. We have seen a combination of different Steganography methods and cryptography method and their measured performance using PSNR and MSE values. The ECC-LSB [2] technique provided better results compared to the other methodology combination. There can be more improvement in the approach of the LSB technique

3 IMPLEMENTATION AND RESULTS

3.1 Encryption Algorithm

1. AES(Advanced Encryption Standard)
   AES means Advanced Encryption Standard which is known as a symmetric block cipher that encodes and decodes the message. In order to encrypt the message in 128 bits, it uses different keys 128 bit, 196-bit,256 bit. It has four stages among which one is a permutation and three are substitution: -

2. **Triple DES**
   DES is known as a symmetric key block cipher that uses DES cipher three times. The first key (k1) is encoded and by using the second key
   (k2) encryption is removed, and then the third key (k3) is written. There is also a difference between the two keys but k1 and k3 are the same keys

   This process is divided into the following steps:

1. 64-bit plain text block is taken to start the process of being assigned the first permutation

2. (IP) function.
3. Initial warrant (IP) is then carried out in plain text.
4. Upcoming, initial access (IP) makes two parts of the permitted block, called Left Blank
5. Text (LPT) and Right Blank Right (RPT).
6. Each LPT and RPT move through 16 rounds of the encoded process.

3.2 Hashing Algorithm

A. SHA (Secure Hash Algorithm)

It stands for Secure Hash Algorithm. It is known as a cryptographic hash function that grabs an input and produces an output of 160-bit (20 bytes) hash value called a message digest. This hash value is usually referred to as a hexadecimal number which is 40 digits long. It is designed by the United States National Security Agency.

B. MD5

The one-way cryptographic function that receives the text of a certain length as input also gives a fixed length as the output of the first image output. This 512-bit series is divided into 16 terms made up of 32 bits each and the result of a 128-bit MD value. The calculation of the MD5 alarm number is done separately in sections that process each 512-bit block of data and the value listed in the previous section. The first stage starts with the message grinding values initiated using consecutive hexadecimal numeric values. Each section consists of four messages a digest pass, which changes values in the recent data block and values refined in the previous block. The last value is calculated in the last block suits the MD5 alarm for that block.

C. Time Comparison of Algorithm Technique

In this above Figure 9, we can see that AES is faster than Triple DES for encrypting the message. The time consumed by AES for different sizes of files and each and every time AES is performing better and faster than Triple DES.

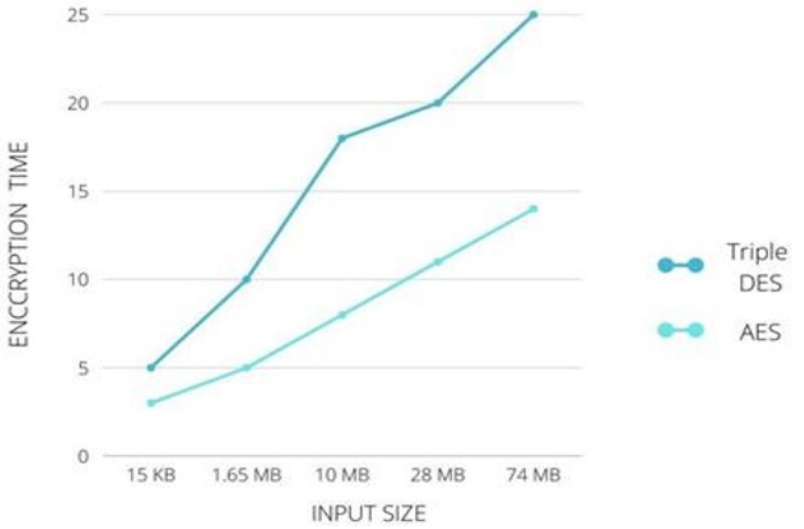

Figure 9:- Encryption time of AES and Triple DES

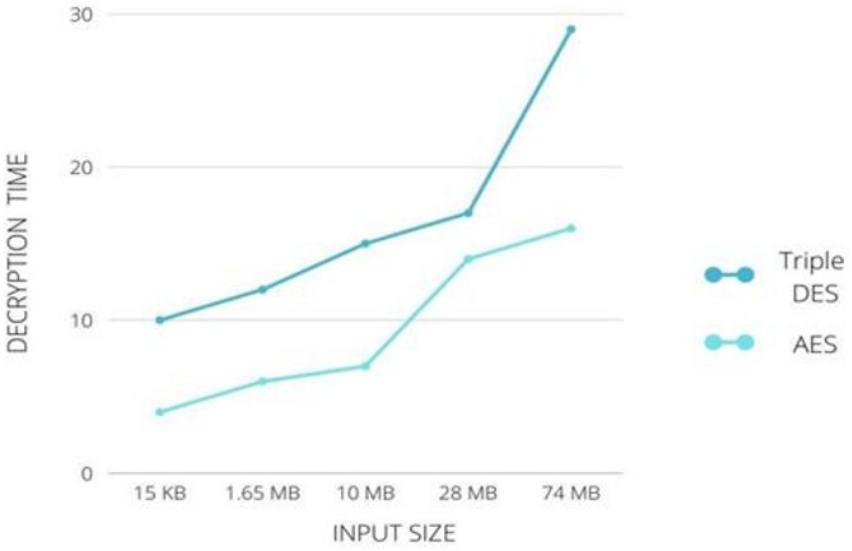

Figure 10:- Decryption time of AES and Triple DES

In decryption Figure 10, we can see that the decryption time taken by AES is faster as compared to Triple DES. The different size of the file is provided and for each file, both decryption method is applied i.e. AES and Triple DES. After providing different sizes of files and comparing both techniques we came to the conclusion that AES is far better for the decryption process. Hence, we can conclude that for both the encryption and decryption process AES is consuming less time and providing better efficiency and accuracy. The Screenshots of the experimental results are as shown in the below figures

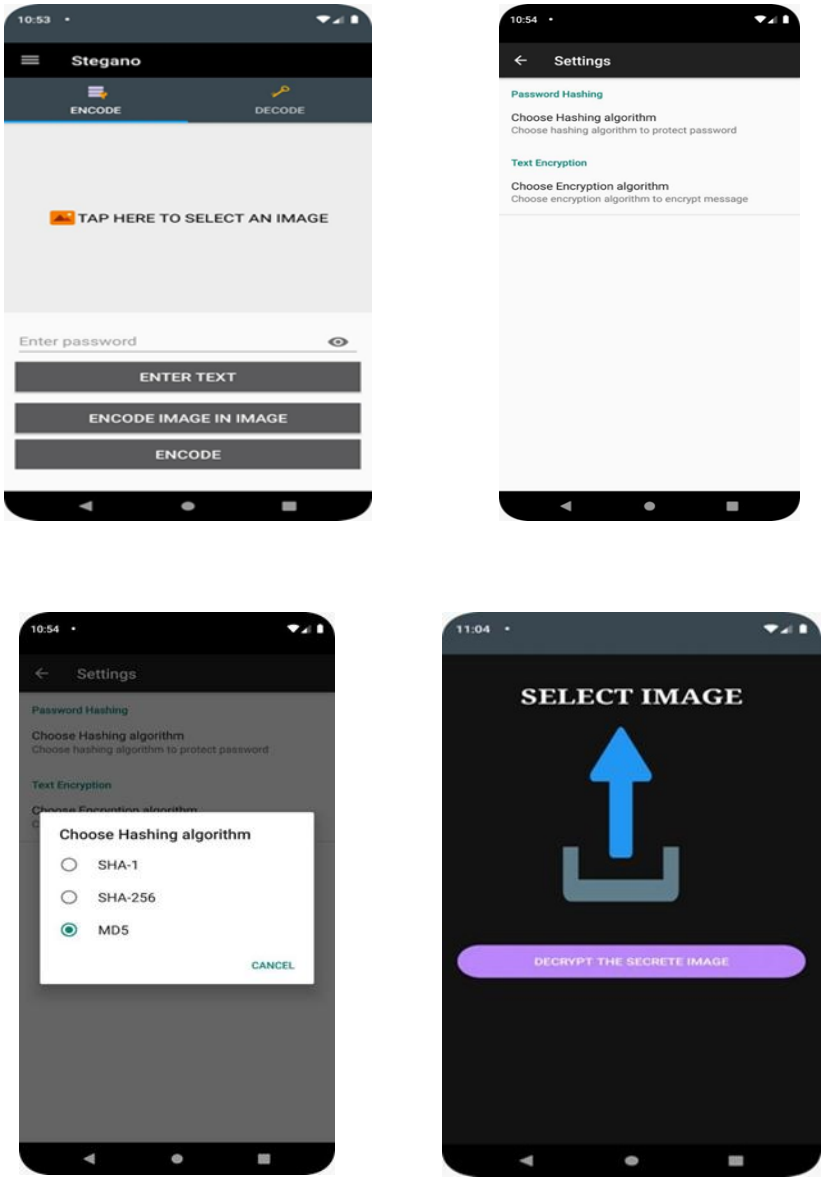

Figure 11: Screenshots of the experimental results

4 CONCLUSION

Steganography is known as the process of hiding the message in any multimedia file in such a way that the attacker cannot know the original information inside it until the authorized access. Similarly, cryptography is the method of encrypting the text by using different algorithms, only the recipient who have key can decrypt it. But from security purpose cryptography is easily cracked by attackers. So here in this project we have tried to combine both the technology stegano and crypto to give our project an advanced level of security. This project not only provides better security but also provides better time efficiency. Its user-friendly environment can give the user a better and rich experience.

We have not only thought of security purposes but this project in the future can be used in IoT of applications. Using different encryption algorithms along with the LSB technique providing the user to select the password hashing option so that their key can be more unique as they want, makes this project completely different from others application present. This project is ready for any future changes and further additional requirements according to the demand of the people and the latest technology available. The project can be used for medical purposes and security purposes. In the future, this project can be embedded with machine learning and data sets to make it more realistic and developed for real-world problems. It can be combined with cloud computing providing it more security and protecting it from all vulnerabilities.

References

1. K. Joshi, "A New Approach of Text Steganography Using ASCII Values." pp. 490–493, 2018.
2. Shivani, V. K. Yadav, and S. Batham, "A Novel Approach of Bulk Data Hiding using Text Steganography," Procedia Comput. Sci., vol. 57, pp. 1401–1410, 2015, doi: 10.1016/j.procs.2015.07.457
3. S. Roy and M. Manasmita, "A novel approach to format based text Steganography," ACM Int. Conf. Proceeding Ser., no. May, pp. 511–516, 2011, doi: 10.1145/1947940.1948046.
4. P. Srilakshmi, C. Himabindu, N. Chaitanya, S. V. Muralidhar, M. V. Sumanth, and K. Vinay, "Text embedding using image Steganography in spatial domain," Int. J. Eng. Technol., vol. 7, no. 3.6, p. 1, 2018, doi: 10.14419/ijet.v7i3.6.14922.
5. Zhang and H. Zhong, "A text hiding method using multiple-base notational system with high embedding capacity," Proc. - 2014 7th Int. Congr. Image Signal Process. CISP 2014, pp. 622–627, 2014, doi: 10.1109/CISP.2014.7003854.
6. R. J. Mstafa and I. S. Member, "A DCT -based Robust Video Steganographic Method Using BCH Error Correcting Codes," 2016.
7. and L. L. Y. Zhang, M. Zhang, X. Yang, "T itle Video Steganography in the compressed area Seyed Sahand Mohammadi Ziabari January 2017 Table of Contents," no. January. 2017.
8. K. B. Sudeepa, K. Raju, H. S. Ranjan Kumar, and G. Aithal, "A New Approach for Video Steganography Based on Randomization and Parallelization," Phys. Procedia, vol. 78, pp. 483–490, 2016, doi: 10.1016/j.procs.2016.02.092.
9. P. Kumar Bandyopadhyay, "various methods of video Steganography 1 Souma Pal and," no. October, 2018.
10. S. Khosla and P. Kaur, "Secure Data Hiding Technique using Video Steganography and Watermarking," Int. J. Comput. Appl., vol. 95, no. 20, pp. 7–12, 2014, doi: 10.5120/16708-6861.
11. Volkhonskiy, I. Nazarov, and E. Burnaev, "Steganographic Generative Adversarial Networks," no. June, 2017.
12. X. Zhou, W. Gong, W. Fu, and L. Jin, "An improved method for LSB based color image Steganography combined with cryptography," 2016 IEEE/ACIS 15th Int. Conf. Comput. Inf. Sci. ICIS 2016 - Proc., pp. 4–7, 2016, doi: 10.1109/ICIS.2016.7550955.
13. J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding data with deep networks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell.

Lect. Notes Bioinformatics), vol. 11219 LNCS, pp. 682–697, 2018, doi: 10.1007/978-3-030-01267- 0_40.
14. R. Hegde and S. Jagadeesha, "Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique," Int. J. Recent Innov. Trends Comput. Commun., vol. 3, no. 7, pp. 4415–4420, 2015.
15. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognit. Lett., vol. 24, no. 9–10, pp. 1613–1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.
16. Kumar and Anuradha, "Enhanced LSB technique for audio Steganography," 2012 3rd Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2012, no. July, pp. 26–29, 2012, doi: 10.1109/ICCCNT.2012.6395978.
17. P. Johri, A. Kumar, and Amba, "Review paper on text and audio Steganography using GA," Int. Conf. Comput. Commun. Autom. ICCCA 2015, pp. 190–192, 2015, doi: 10.1109/CCAA.2015.7148403.
18. Sazeen et al., "A novel Steganography approach for audio files A Novel Steganography Approach for Audio Files," pp. 0–14, 2020.