A HYBRID APPROACH FOR IMAGE SECURITY BY COMBINING ENCRYPTION AND STEGANOGRAPHY

[1]G. Gayathri, [2]CH. Sampath, [3]A. Aditya, [4]P. Sunil Kumar, [5] A. Akhilesh
[1]Assistant Professor, [2,3,4,5]Student
[1]Department of Computer Science & Engineering,
[1]Anil Neerukonda Institute Of Technology And Sciences, Visakhapatnam, India.

ABSTRACT

Cyber crime has become a dangerous threat to all the technical users and layman. Due to lack of skill on using the secured means in the data communication, many users as well as organizations are suffering. As we know that India is moving a step ahead in technical aspects, which is enhancing and improving the concept "Digital India", but we must intensify the concept to "Secure Digital India" where we can see no data breaches, no malicious attacks and no cyber terrorism. Security in transmission through the public channels, storage of digital images has its importance in today's image communications and confidential video conferencing. Because of expanding use in sharing the images in the daily social life, it is essential to protect the confidential image data from unauthorized access. Advanced Encryption Standard (AES), a block cipher based algorithm is a well famous methodology making several advantages in data encryption. We are doing a hybrid approach for image security that combines both encryption of the image data and hiding the encrypted data into another image through steganography. The research helps layman to share the images into the public channels without getting compromised.

Keywords – Cryptography, Steganography, Encryption, Decryption, AES, LSB, Hiding-Extracting, Cyber security, Image security, Cyber threats.

1. INTRODUCTION

Cyber Security is the body of technologies, whose processes and practices are drafted to protect networks. Apart from detecting the already existing threat, it also uses the intrusion prevention methods, in order to avert the upcoming threats.
In order to avert threat, virus or any unauthorized access into a network or a computer, we need to safeguard the network with a firewall and awareness of hacking. It is important to avert security breach which can cause diminution for an organization. Potential threats like loss, modification, unauthorized access, data leak must be prevented.

1.1 Cryptography

To verify that the confidentiality, integrity and availability of data , it's vital to secure the knowledge. One pivotal branch of information security is cryptography, the science of securing the data. Cryptography permits the original data to be converted into cipher data that can be sent over the unsecure channel. Fig.1. shows the representational diagram of the steps followed by sender and receiver using cryptography. Encryption is the procedure of transforming the native data into cryptographic data so that only intended recipient can decipher the data by applying decryption.

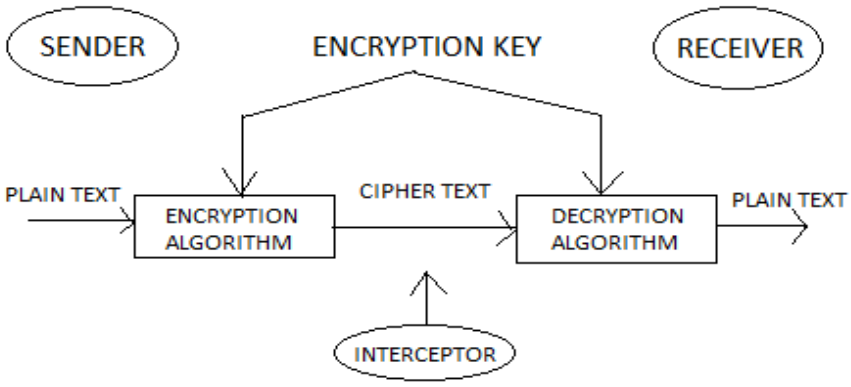

Fig. 1 Cryptography

1.1.1 Symmetric / Secret Key Cryptography

The strategy of Secret key (same to sender and receiver) encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all side's encryption and decryption secret data. The first information or plaintext is encrypted with a key by the sender side also, an equivalent key's employed by the receiver to decrypt the encrypted data to get the plaintext. The key will be known only by the people who are legitimize to the modules of encryption/decryption. However, the technique pledges the good security for transmission but there is a difficulty with the distribution of the key. if one nab or explore the key he can get whole data without any difficulty. A case of Symmetric Key cryptography approach is DES Algorithm.

1.1.2 Asymmetric / Public Key Cryptography

We can call this system as the asymmetric cryptosystem or public key cryptosystem, this uses two keys which are mathematically associated, use separately for encrypting and decrypting the knowledge. During this technique, once we use the private key, there are not any possibilities to get the info or just discover the opposite key, all keys are needed for the technique to run. The key used for encryption is stored public, ergo it's called public key, and therefore the decryption key's stored secret and called private key. An example of Asymmetric-Key Algorithms is RSA.

1.2 Steganography

Steganography is the branch of information security that enables the information hiding. It is the art and science of hiding the data within a cover in order to avoid disruption, modification and disclosure etc. Steganography differs from cryptography in the sense that it keeps the existence of information secret while cryptography keeps contents of information secret. Embedding is the process of hiding a secret message within a cover. A great deal of attention is required so that secret message goes unnoticed if third party intercepts the message. Extracting is the inverse of embedding process where secret message is revealed at the end.

2. LITERATURE REVIEW

2.1 Related Work

In [4], proposed an encrypting technique by combining cryptography and steganography techniques to cover the info . In cryptography process, they proposed an efficient technique for encoding using one's complement method, which we called as SCMACS. It used a symmetric key method where both sender and receiver share an equivalent key for encryption and decryption. In steganography part, we used the LSB method that's used and mostly preferred.

In [5], authors proposed a highly secured steganography technique by combining DNA sequence with Hyperelliptic Curve Cryptography. This approach executes the benefits of both techniques to afford a high level of security communication. Also, it uses the advantages of both DNA cryptography and Steganography. This algorithm tries to cover a secret image in another cover image by convert them into DNA sequence using the nucleotide to the binary transformation table. On the sender side, the embedding method includes three steps. First, they convert the values of a pixel of both the duvet image and secret image to their respective DNA triplet value utilizing characters to the DNA triplet conversion. Secondly, they convert the triplet values to binary values format. within the end , apply the XOR logic between binary values of both secret image and canopy image to get a replacement image which called stego image.

In [6], authors presented a replacement technique called multi-level secret data hiding which integrates two different methods of encryption namely visual cryptography and steganography. After that visual cryptography is performed that produces the shares which form the first level of security then steganography during which thy used the LSB method to hide the shares in several media like image, audio, and video.

The paper at [7] presented a way supported combining both the strongencrypting algorithm and steganographic technique to form the communication of tip safe, secure and very hard to decode. An encryption technique is used for encrypting a secret message before encoding it into a QR code. UTF-8 format is converted into base64 format to form it compatible for further processing. The encoded image is scrambled to realize another security level. The scrambled QR code is finally embedded during a suitable cover image, which is then transferred securely to deliver the key information. They utilized a least significant bit method to accomplish the digital image steganography. At the receiver's side, the key data is retrieved through the decoding process. Thus, a four-level security has been rendered for them a secret message to be transferred.

In [8] authors presented a picture steganography method. At first, they used the DES algorithm to encrypt the text message. They used a 16 round and with block size 64-bit. then the K-Means Clustering of The Pixels method which clusters the image into numerous segments and embedded data in every segment. There are many clustering algorithms use for image segmentation. Segmentation includes an enormous set of data within the sort of pixels, where every pixel additional has three components namely red, green and blue(RGB). After the formation of clusters, the encrypted text is separated into K number of segments. These segments are to be hidden in each cluster. They used the LSB (Least Significant Bit) method for this purpose.

In [9], authors presented a way to increase the embedding capacity and to enhance the standard of stego image. The Adaptive Pixel Value Differencing which is an improved sort of Pixel Value Differencing was utilized because the Steganographic system although AES was utilized because the Cryptographic system. during this method, they used a picture as a canopy to cover the key data inside. This cover should be a grayscale image. therefore, pixel size must be 256*256. If the dimensions of a pixel was high, they brought it to the present range. They checked if the duvet image may be a colour image they changed it into the grayscale range. They used APVD algorithm to embed the info into the duvet image. The result gotten after hiding the info called stego image. They used AES algorithm to encrypt stego image.

In [10], authors conducted a performance analysis survey on various algorithms like DES, AES, RSA combining with LSB substitution technique which serves well to draw conclusions on the three encryption techniques supported their performances in any application. it's been concluded from their work that AES encryption is best than other techniques because it accounts for fewer encryption, decryption times and uses less buffer space.

In [11], authors performed a contemporary method during which use Huffman encoding to hide data. They took a gray level image of size m*n as cover image and p*q as a secret image. then, they executed the Huffman encoding over the key image and each little bit of Huffman code of a secret image is hidden into a canopy image utilizing LSB algorithm.

2.2 Steganography vs Cryptography

Steganography and Cryptography are used for the purpose of data transmission over an insecure network without the data being exposed to any unauthorized persons. Steganography embeds the data in a cover image while cryptography encrypts the data. The advantage of steganography is that the look of doubt for the attacker to suspect the file isn't changed and ibis it will not raise any that there may be some data hidden unlike cryptography that encrypts the data and sends it to over the network.

2.3 Combination of Steganography and Cryptography

It is noted that steganography and cryptography alone is insufficient for the safety of data, therefore If we combine these systems, we will generate more reliable and powerful approach.
The combination of these two strategies will enhance the safety of the knowledge secret. This combined will fulfill the prerequisites, for instance, memory space, security, and strength for important information transmission across an open channel.
Also, it'll be a strong mechanism that enables people to speak without interferes with eavesdroppers even knowing there's a method of communication within the first place.

2.4 AES Algorithm

Advanced Encryption Standard is a symmetric block cipher encryption algorithm that uses a single key to encrypt the data.

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes except for the last and final round of the algorithm. In the last round of the AES algorithm we will remove one of the transformation called mix column transformation. The first round process is depicted below.

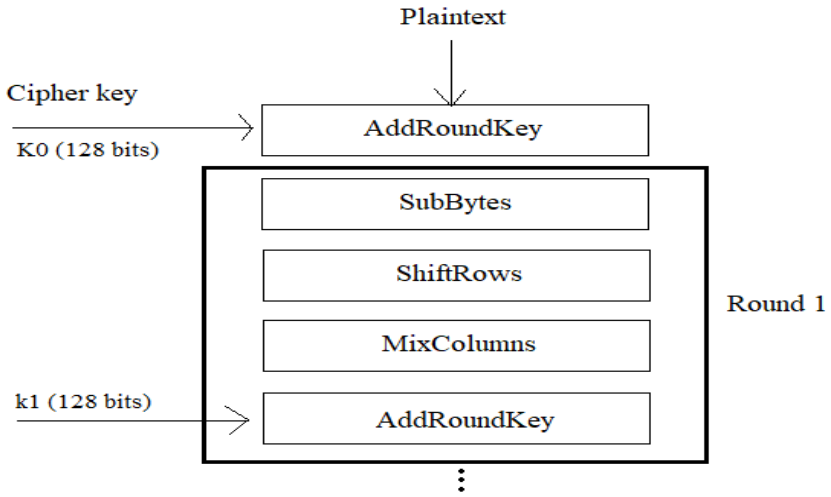

Fig. 2 AES round

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a tough and fast table (S-box) given in design. the result is during a matrix of 4 rows and 4 columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left(except the 1st one). Any entries that 'fall off' are re-inserted on the right side of row. Shift is run as follows −

1. First row isn't shifted

2. Second row is shifted one(byte) position to the left

3. Third row is shifted two positions to the left

4. Fourth row is shifted three positions to the left

The result's a replacement matrix consisting of the same 16 bytes but shifted with regard to each other .

MixColumns

Each column of 4 bytes is now converted employing a special function . This function takes as input the four bytes of 1 column and outputs four completely new bytes, which replace the primary column. the result is another new matrix consisting of 16 bytes. It should be noted that this step isn't performed within the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is often often the last round then the output is that the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes which we start another similar round.

Decryption Process

The process of decryption of an AES ciphertext is analogous to the encryption process within the reverse order. Each round consists of the four processes conducted within the reverse order −

1. Add round key

2. Mix columns

3. Shift rows

4. Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms must be separately implemented, although they're very closely related.

2.5 LSB Technique

Images are ideal for information hiding due to the massive amount of dispensable space is made within the storing of images.
The most common and popular method of modern-day steganography is to form use of LSB of picture's pixel information. This system works best when the file is longer than the message file and if image is graysscale. When applying LSB techniques to every byte of a 24bit image, three bits are often encoded into each pixel. If the LSB of the pixel value of canopy image C(i,j) is adequate to the message bit SM of secret message to be embedded, C(i,j) remain unchanged, if not set the LSB of C(i,j) to SM.
Message embedding process is given:
S(i,j) = C(i,j) – 1, if LSB(C(i,j)) = 1 and SM = 0.
S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and SM = 1.
S(i,j) = C(i,j) , if LSB(C(i,j)) = SM

Where LSB(C(i,j)) stands for the LSB of canopy image C(i,j) and "SM" is that the next message bit to be embedded. S(i,j) is that the stego image. Many variations of this LSB algorithm are often used one such example is given below-

We can use images to hide things if we replace the last bit of every colors byte with a bit from the message.
Message A- 01000001
Image with 3 pixels

Pixel 1: 11011000	11001001	00000011
Pixel 2: 11011000	11001001	00000011
Pixel 3: 11011000	11001001	00000011

Now we hide our message in the image.
Message: 01000001

Pixel 1: 1101100**0**	1100100**1**	0000001**0**
Pixel 2: 1101100**0**	1100100**0**	0000001**0**
Pixel 3: 1101100**0**	1100100**1**	00000011

3. METHODOLOGY

3.1 Real-Time Problem Solution

The intrinsic issue with the image security in today scenario is, there's no proper secured channels through which the image are often sent from the sender to the receiver. Therefore the modules in our present provides the integrity and confidentiality to the users by using the mixture of encryption and hiding the image.

3.2 System Architecture

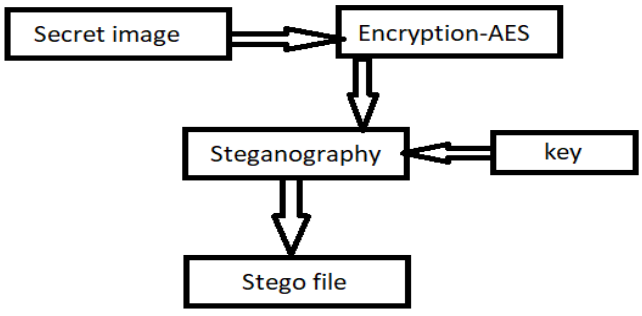

Fig. 3 Sender side

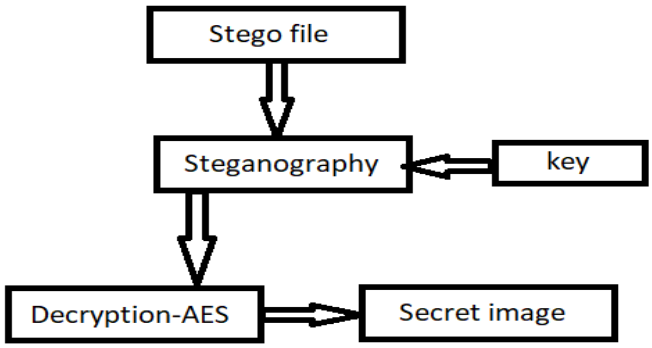

Fig. 4 Receiver side

At the sender the received secret image is encrypted using the symmetric algorithm AES with a personal key. Further the encrypted data of the image is hidden inside the duvet image using the steganographic method LSB.
In a similar way the key image is extracted from the duvet image within the receiver side.

3.3 Module Division

There are three modules within the methodology.

1. Image-Hexdata
2. Encryption-Decryption
3. Hiding-Extracting

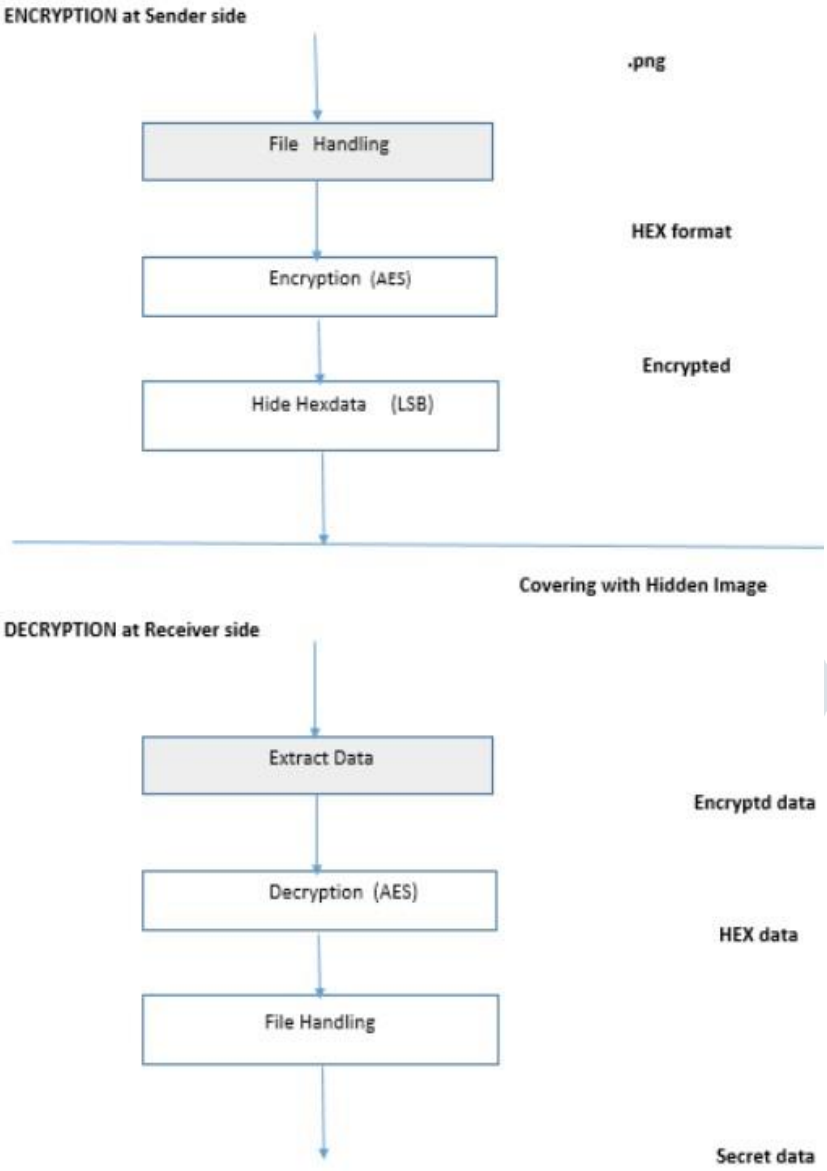

Fig. 5 Module flow

Image-Hexdata

In this module the image data is converted into the Hex format at the sender side to supply the info to the encryption algorithm for encryption.
Similarly, at the receiver side the hexdata is converted because the image format .

Encryption-Decryption

In this module the hex data generated at the sender side is encrypted using the AES algorithm.
And the extracted data,(i.e. encrypted) at the receiver side is then decrypted using the decryption AES algorithm.

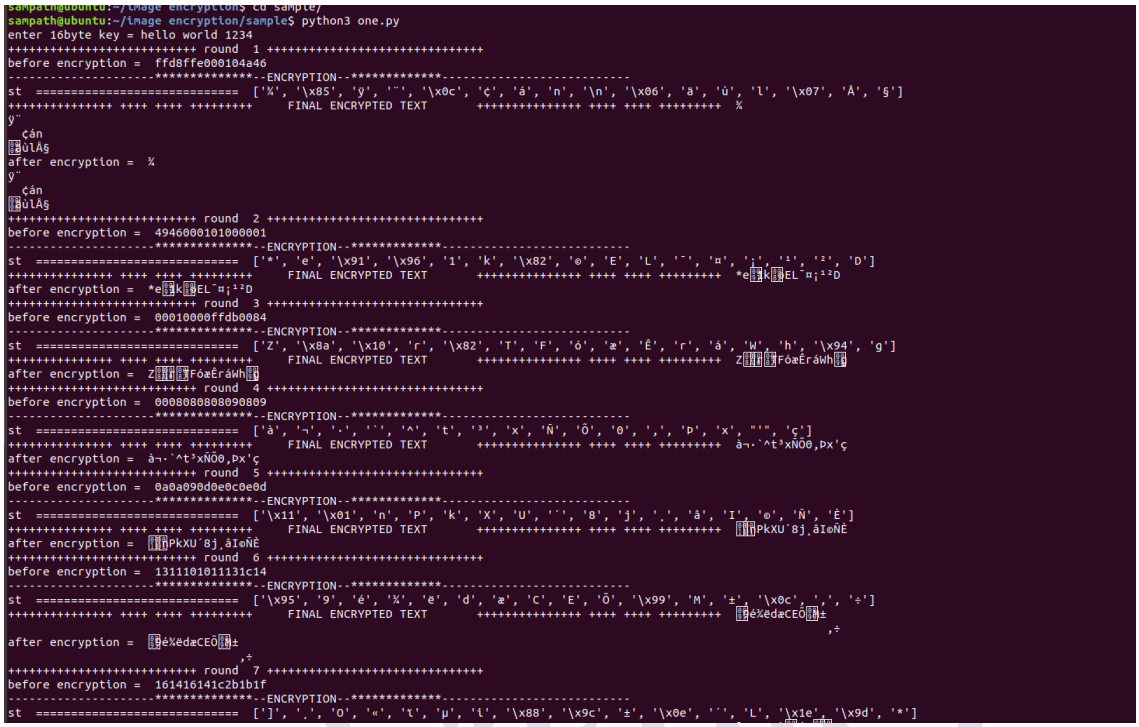

Fig. 6 Encryption

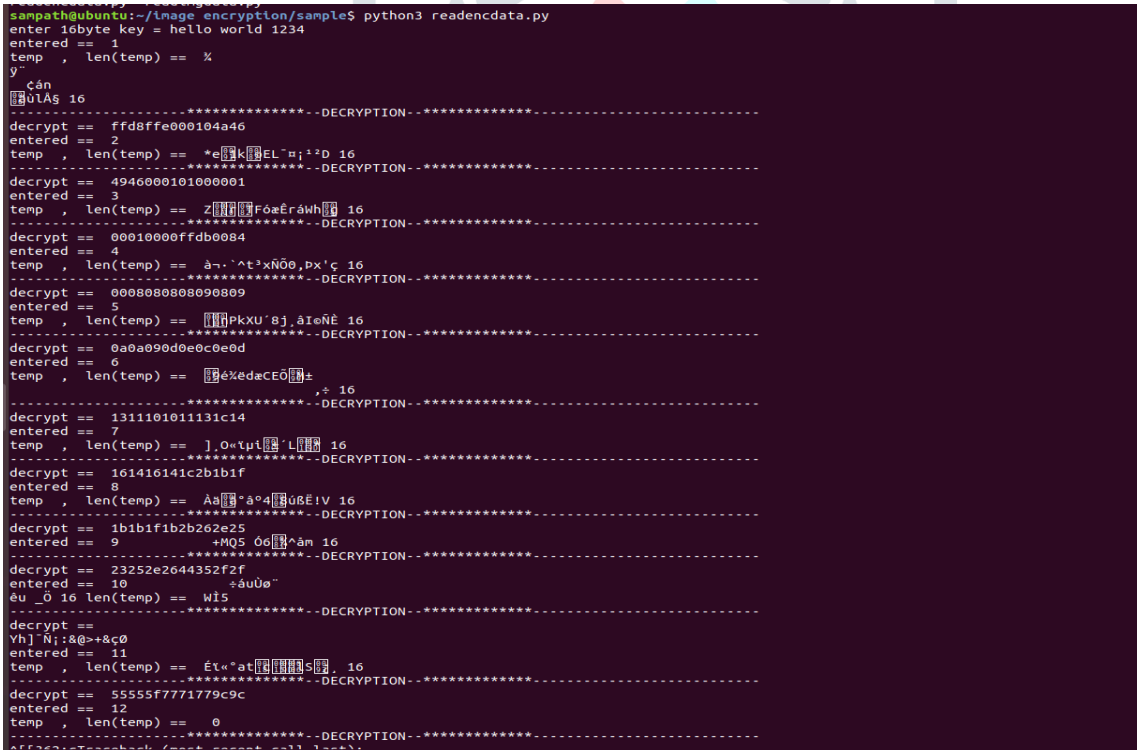

Fig. 7 Decryption

Hiding-Extracting

In this module the encrypted data from the AES encryption algorithm is stored inside the duvet image using the LSB steganographic method.

And at the receiver side the encrypted data is extracted from the duvet image using the LSB extraction method.

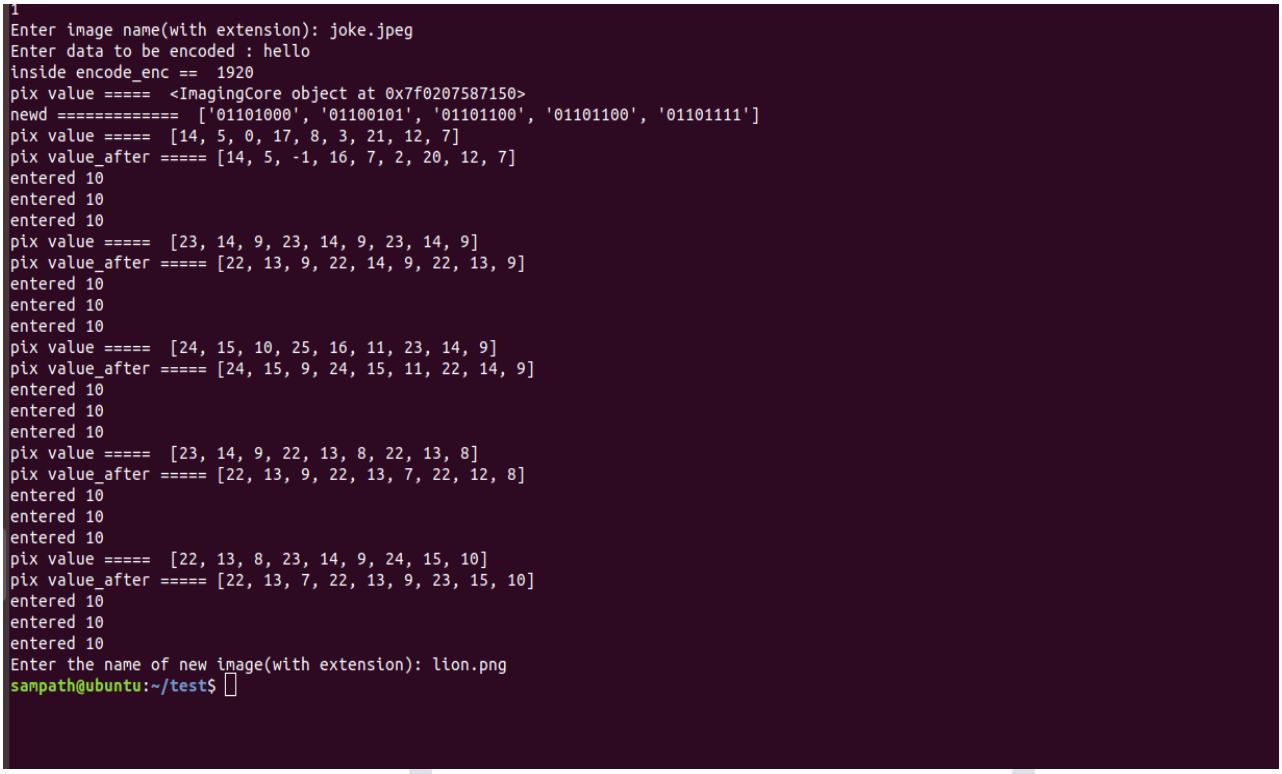

Fig. 8 Steganography

4. CONCLUSION

In this project, we've taken the matter of sharing the pictures within the public channels. It is known that the layman to technology uses the general public channels aren't secured to the extent to satisfy the confidentiality and integrity to the user. Many steganography methods are been used to hide the secret images inside the cover images that are been transmitted into the insecure channels. However, using the steganographic methods alone may lead to extraction of the secret images with the known method of hiding. Hence, in this project we have used the combined method of hiding the encrypted image into the cover image. Therefore, even in the scenario where the hacker can extract the hidden data, fails to decrypt the data to form the original secret image. By consolidating the two methods of cryptography and steganography, the safety of image transfer through the insecure channels is achieved.

5. REFERENCES

[1] J. K. Saini and H. K. Verma, “A hybrid approach for image security by combining encryption and steganography,” in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on IEEE, 2013, pp. 607–611.

[2] P. Kumar and V. K. Sharma, “Information security based on steganography & cryptography techniques: A review,” International Journal, vol. 4, no. 10, 2014.

[3] H. Sharma, K. K. Sharma, and S. Chauhan, “Steganography techniques using cryptography-a review paper,” 2014.

[4] A. Dhamija and V. Dhaka, “A novel cryptographic and steganographic approach for secure cloud data migration,” in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 346–351.

[5] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, “An improved level of security for dna steganography using hyperelliptic curve cryptography,” Wireless Personal Communications, pp. 1–22, 2016.

[6] S. S. Patil and S. Goud, “Enhanced multi level secret data hiding,” 2016.

[7] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, “Enhanced security in steganography using encryption and quick response code,” in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016, pp. 2308–2312.

[8] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering and encryption techniques," in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016, pp. 1206–1211.

[9] F. Joseph and A. P. S. Sivakumar, "Advanced security enhancement of data before distribution," 2015.

[10] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution," IJSR, India, 2013.

[11] R. Das and T. Tuithung, "A novel steganography method for image based on huffman encoding," in Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on. IEEE, 2012, pp. 14–18.

[12] K. Muhammad, J. Ahmad, M. Sajjad, and M. Zubair, "Secure image steganography using cryptography and image transposition," arXiv preprint arXiv:1510.04413, 2015.

[13] S. E. Thomas, S. T. Philip, S. Nazar, A. Mathew, and N. Joseph, "Advanced cryptographic steganography using multimedia files," in International Conference on Electrical Engineering and Computer Science (ICEECS-2012), 2012.

[14] A. Gambhir and A. R. Mishra, "A new data hiding technique with multilayer security system." 2015.

[15] M. H. Sharma, M. MithleshArya, and M. D. Goyal, "Secure image hiding algorithm using cryptography and steganography," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, pp. 2278–0661, 2013.

[16] Seyed Hossein Kamali, Reza Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", IEEE Electronics and Information Engineering International Conference (ICEIE 2010). 1-3 Aug. 2010, V1- 141 – V1-145.

[17] Ahmed AL-Shaaby, Talal AlKharobi "Cryptography and Steganography: New Approach".