ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (80-88), Month: July - September 2016, Available at: www.researchpublish.com

Effective AES Cryptography and Pixel Value Differencing Steganography Techniques for Secure Data Transmission

Ms. Suchitra B[1], Ms. Anita Madona M[2]

[1]M.Phil Research Scholar, [2]Assisant Professor, Department of Computer Science Auxilium College (Autonomous), Vellore, Tamilnadu, India

Abstract: **As digital information and data are transferred over the internet and securing sensitive messages need to discover and developed more often than even before. So new technologies for protecting and securing the sensitive messages need to realize and develop. Here we were using the cryptography and Steganography techniques to hide the information from source to destination in a secure manner. Cryptography and Steganography are the two important methods for secure communication. In this proposed system we develop highly secure model by combining AES cryptographic security and LSB Steganography security. In cryptography we are using Advanced Encryption Standard (AES) algorithm to encrypt secret message that is to convert plain text to a cipher text. Then Pixel Value Differencing (PVD) with K-bit LSB (Least-Significant-Bit) substitution is used to hide the cipher text into true color RGB image. Our proposed model gives security at two levels to sensitive information.**

Keywords: **Cryptography, Steganography, AES algorithm, PVD Method.**

I. INTRODUCTION

As the production, storage and exchange of information becomes more extensive and important in the functioning of societies, the problem of protecting the information from unintended and undesired use becomes more complex. In modern societies, protection of information involves many interdependent policy and technological issues relating to information confidentiality, integrity, anonymity, authenticity, utility, etc.

So we need some security techniques to save the information from hackers, the two security techniques used are cryptography and Steganography. Cryptography was created as a technique for securing the secrecy of communication and with different methods developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secrecy. The technique used to implement this, is called Steganography. Cryptosystem proves as a unique security solution in various emerging applications concerned to electronics, communication, networks where security is necessary.

The advance security is not sustained by the password security but is achieved by hiding the existence of information, which can be done by Steganography. Steganography systems can hide message inside of digital objects such as file that has been hidden inside a digital picture, video or audio file. The Steganography and cryptography is used to guarantee the security of the secret message.[1]in this paper DES cryptography and LSB Steganography method is described, by improving the LSB method, so as to hide large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method.[2]in this paper they describe about a technique based on the advanced LSB and RSA algorithm, RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission.[3] in this paper they purpose a high performance LSB Steganography method, the LSB insertion is applied to hide data inside an image because it is considered as more secure and attractive.[4] In this paper a DCT based

watermarking scheme is proposed which provides higher resistance towards image processing attacks such as JPEG compression, noise, rotation, translation etc.[5] in this paper they described about the different types of symmetric key cryptography algorithms, how to transfer the information from source to destination in a secure manner.

II. PROPOSED SYSTEM

The main objective of this research is protecting and securing the information from hackers when it sends from source to destination. Three general goals defined for security are confidentiality, integrity and availability, two types of attacks threaten the confidentiality of information they are snooping and traffic analysis, four types of attacks can threaten the integrity of information they are modification, masquerading, replaying and repudiation, denial of service attacks threaten the availability of information. So to protect the information from attackers and to communicate the information in a secure manner we combine two techniques cryptography and Steganography.

Cryptography is used to encrypt the message from plain text to cipher text using AES algorithm, and Steganography is used to embed the cipher text in image using k-bit LSB and PVD techniques, this both techniques help the user to send the data in a secure manner in AES we were using 128 bits which was more secure than 192 and 256 bits, because till now no threats were found on 128 bits, but threaten found on 192 and 256 bits.

A. Cryptography

Cryptography is an art of transmitting the data safely over the internet by applying some cryptographic algorithms so that it will be difficult for an attacker to attack or steal some confidential or private information. There are two types of encryption algorithms: symmetric encryption algorithm and asymmetric encryption algorithm. In symmetric key encryption sender and receiver will have the same key for the process of encryption and decryption of data. In asymmetric key encryption algorithm different keys are used in sending and receiving site for encryption and decryption.

AES Algorithm

Advanced Encryption Standard (AES), also known as Rijndael, is used for securing information. Unlike its predecessor DES, AES does not use a Feistel network. The AES algorithm is a symmetric key block cipher with a block length of 128 bits and it support for key lengths of 128 or 192 or 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used for encryption as well as decryption of a message. AES is based on a design principle known as a Substitution permutation network.AES operates on bytes of a 4×4 matrix, termed the state. The Advanced Encryption Standard cipher is specified as a number of repetitions of transformation rounds that converts the input plaintext message into the final output of cipher text message. Each round in AES consists of several processing steps, which depends on the encryption key. A set of reverse rounds are applied to decrypt encoded cipher text back into the original plaintext message using the same encryption key. Advantages of AES algorithm is security, reasonable cost along with the main characteristics of flexibility and simplicity.

AES structure is as follows:

1. Data block of 4 columns of 4 bytes is state.
2. Key is expanded to array of words.
3. Has 9/11/13 rounds in which state undergoes:

- byte substitution (1 S-box used on every byte)
- shift rows (permute bytes between groups/columns)
- mix columns (subs using matrix multiply of groups)
- add round key (XOR state with key material)
- view as alternating XOR key & scramble data bytes

4. Initial XOR key material & incomplete last round
5. With fast XOR & table lookup implementation.

B. Steganography

Steganography comes from the Greek word that literally means "secret writing or covered". Nowadays in this modern globe privacy, safe and secrecy is must for the internet users. The former uses of Steganography are for conveying the top secret files and documents among worldwide governments. The mainly used method today for hiding the covert msg into a digital image is Steganography. The Steganography method takes advantage of the weakness of the Human Visual System. The persons cannot easily find the hidden information in the image. The vital objective of Steganography is to hide the data from the attackers view and securely transmit the data over the image from source to destination. In Steganography the image is classified into two types cover image and Stego image. The cover image is an original image and the Stego image is after hiding the message into the original image.

PVD and K-bit LSB Steganography

The Pixel-Value Differencing (PVD) method is proposed by Wu and Tsai to successfully provide both high embedding capacity and outstanding imperceptibility for the Stego images. In Pixel-Value Differencing (PVD) Steganography method, first the cover image is partitioned into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A small difference value can be located on a smooth area and the large one is located on an edged area. From the aspect of human vision it has a larger tolerance that embeds more data into edge areas than smooth areas. PVD and *K*-bit LSB replacement method provides larger embedding capacity and higher image quality. It provides an easy way to produce a more imperceptible result than simple LSB replacement methods. The embedded secret message can be extracted from the resulting Stego image without referencing the original cover image.

Advantages of using PVD and K-bit LSB Steganography: Gives high data embedding capacity and provides high imperceptible quality Stego images with high security.

III. CRYPTO-STEGANOGRAPHY TECHNIQUES

To secure information against security breaches and attacks there is a need for more sophisticated techniques of protecting secret data. To avoid the problem of unauthorized data access Steganography along with cryptography seems to be an appropriate solution. By combining both the techniques, more robust security can be achieved. Cryptography scrambles a message that cannot be understood; Steganography hides the message so that it cannot be seen. A cipher message for instance, might arouse case of investigation on the part of the recipient while an invisible message created with Steganography method will not be so. The major difference between the two is that cryptography protects the content of a message and Steganography protects, hide the message and the communicating parties.

In this paper we had combined cryptography and Steganography to give two tier securities to secret data. First the message is encrypted by using Advance Encrypted Standard (AES) encryption algorithm. Then encrypted message is embedded into cover image by using PVD Steganography and K-bit LSB substitution method.

A. Block Diagram of Crypto-Steganography Encryption and Embedding Algorithm

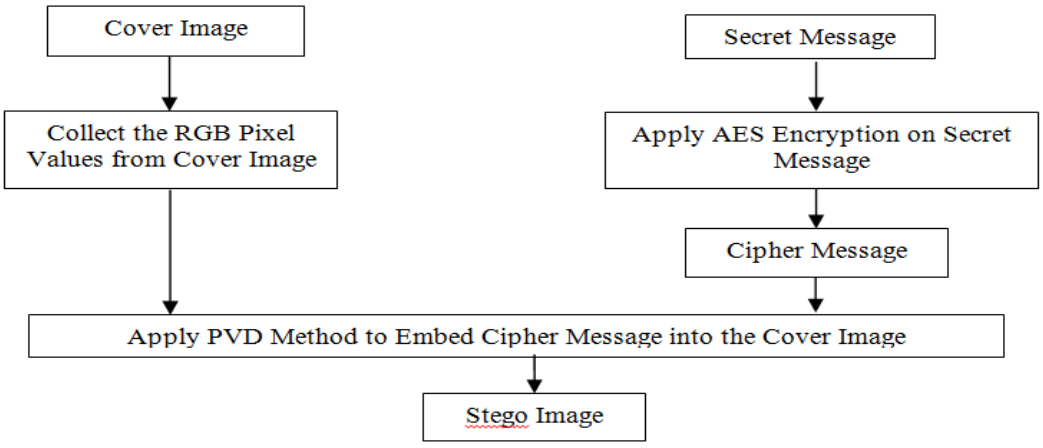


Fig 1: crypto-Steganography encryption and embedding procedure

Fig 1 explains the crypto-Steganography encryption and embedding procedure, first the secret message will be encrypted using cryptography AES algorithm, then the encrypted message will be embedded into the cover image using PVD with K-bit LSB technique, to get a Stego image.

Encryption and Embedding Algorithm

Encryption Procedure

AES (plaintext, key)

Step 1: start.

Step 2: round ←14.

Step 3: state [1] ← first four bytes of the plaintext.

Step 4: state [2] is assigned with next four bytes and so on.

Step 5: call addroundkey (state, key)

Step 6: repeat steps 7 to 10 while rounds is 1 to 14.

Step 7: call Sub Bytes (state)

Step 8: call Shift Rows (state).

Step 9: call Mix Columns (state).

Step 10: call addroundkey (state, key).

Step 11: return the value of state.

The AES algorithm takes the input of plaintext and key. Round is assigned with the value 4 as 4*4 matrixes are used. Each and every state is assigned with the four bytes of the plaintext. For each round all the four stages of AES are called.

Embedding Procedure

Inputs: Encrypted Secret Data (D), Cover Image(C)

Output: Stego image(S) with secret data embedded in it.

1. Divide encrypted secret data into three Data blocks D1, D2, D3.

2. Convert the each Secret Data blocks (D1, D2, and D3) into binary format.

3. Split the cover image C into Red, Green and Blue Planes. (R, G and B respectively)

4. Divide Red (R) Plane of cover image into non overlapping blocks of two consecutive pixels.

5. Call PVD and K-bit LSB algorithm to embed encrypted secret data block D1 into Red Plane(R) of cover image.

6. Call PVD and K-bit LSB algorithm to embed encrypted secret data block D2 into Blue Plane (B) of cover image.

7. Call PVD and K-bit LSB algorithm to embed encrypted secret data block D3 into Green Plane (G) of cover image

8. Store the resulting image as Stego Image (S) Block diagram of proposed system for data extraction as Shown in Figure 2.

B. Block Diagram of Crypto-Steganography Decryption and Extraction Algorithm

Fig2 explains the crypto-Steganography decryption and extraction procedure, after the encryption and embedding of the Stego image that will be received by the receiver. Receiver will apply PVD with K-bit LSB method to de-embed the Stego image to get the cipher message, then the cipher message will be decrypted using AES algorithm, finally we will get a secret message.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (80-88), Month: July - September 2016, Available at: www.researchpublish.com

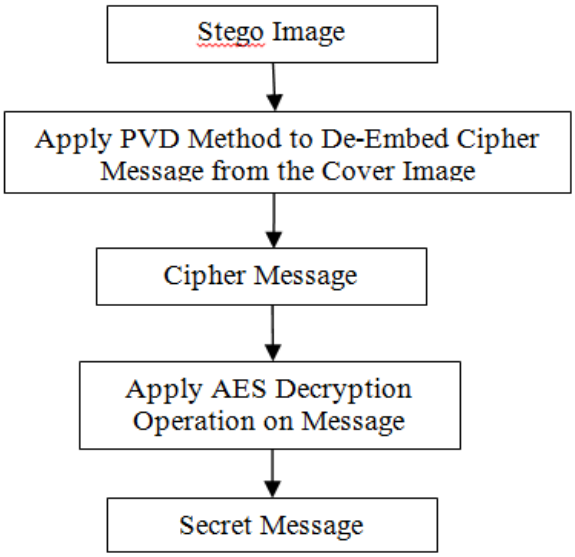


Fig 2: Crypto-Steganography Decryption and Extracting procedure

Decryption and Extraction Algorithm

Decryption Procedure

Step 1: start

Step 2: state [1] ←first four bytes of the plaintext.

Step 3: state [2] is assigned with next four bytes and so on.

Step 4: step 5 to 9 is repeated varying rounds from 1 to 14.

Step 5: addroundkey (state, key).

Step 6: inversesubbytes (state).

Step 7: inverseshiftrows (state).

Step 8: inversemixcolumns (state).

Step 9: return the value of state.

Extraction Procedure

Input: Stego Image(S)

Output: Secret Data (D)

1. Split the Stego image S into Red, Green and Blue Planes(R, G and B respectively).

2. Call PVD and K-bit LSB data extraction Algorithm to extract encrypted secret data block D1 from Red Plane(R) of Stego image.

3. Call PVD and K-bit LSB data extraction algorithm to extract encrypted secret data block D2 from Blue Plane (B) of Stego image.

IV. RESULT AND DISCUSSION

The experimental results are based on various image quality assessment metrics for the performance evaluation. The table 5.1 shows the experimental result of proposed techniques, here the focus is on short messages with length of 150 bytes to 1500 bytes, because they are the most challenging one to detect. And if we save the resultant image in a lossy format like jpeg, the data will be lost. So saving the resultant image as PNG is pretty good, here we had compared the image quality of cover image and Stego image using PSNR and MSE values. Our proposed techniques shows the lesser MSE values,

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (80-88), Month: July - September 2016, Available at: www.researchpublish.com

that is lesser errors that cannot be found by human eye, so our technique is more secure and confident compared to existing techniques.

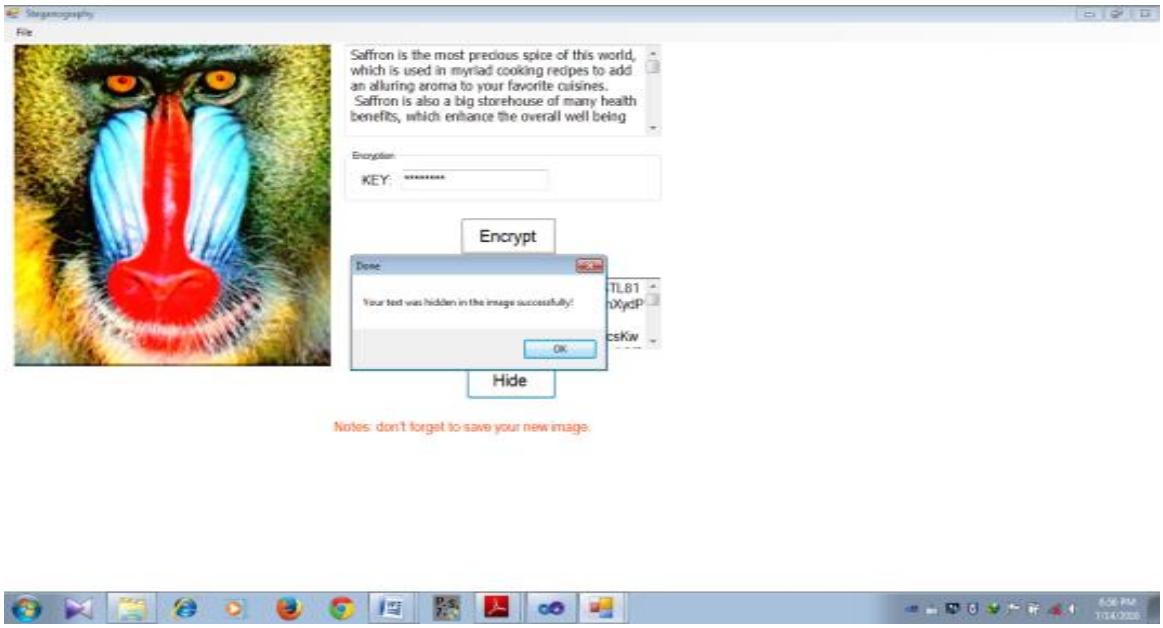
1. Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) measures the estimates of the quality of Stego image compared with an original image and is a very commonly used metric to measure image reliability or conformity.

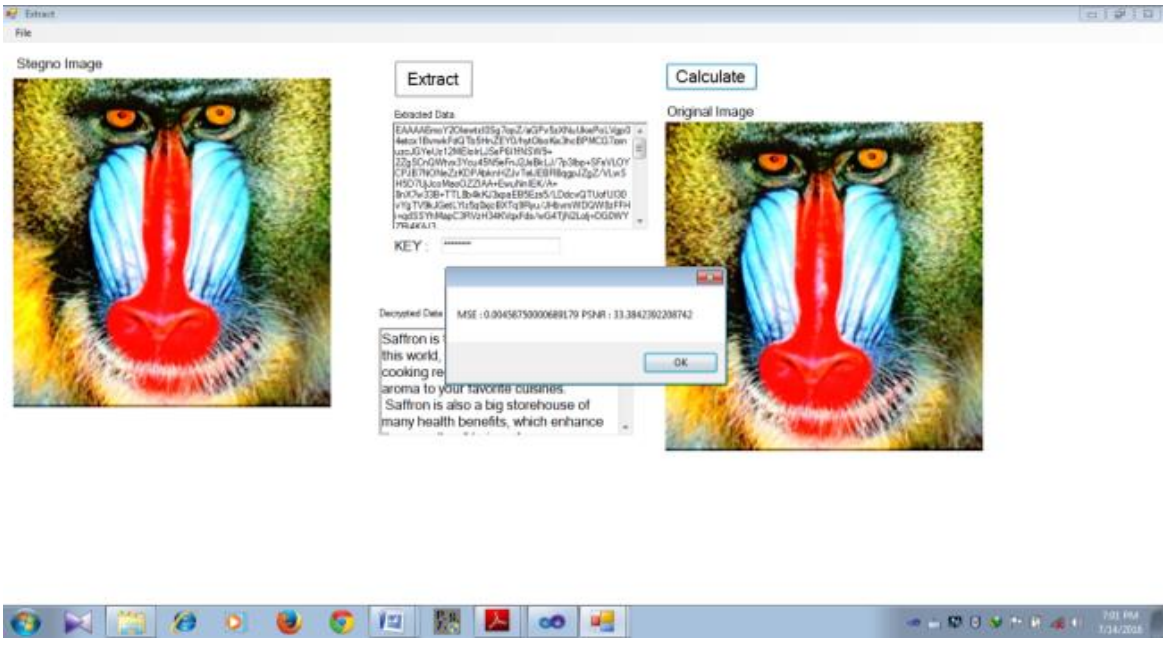
2. Mean Square Error (MSE)

The Mean Square Error is defined as the square of the difference between the pixel values of the original image and the Stego image and then dividing it by size of the image. The mathematical formula for computing Mean Square Error between x and y images of sizes M*N. The lower value of Mean Square Error (MSE) signifies lesser error in the Stego image in other words better quality.

Encryption and Embedding



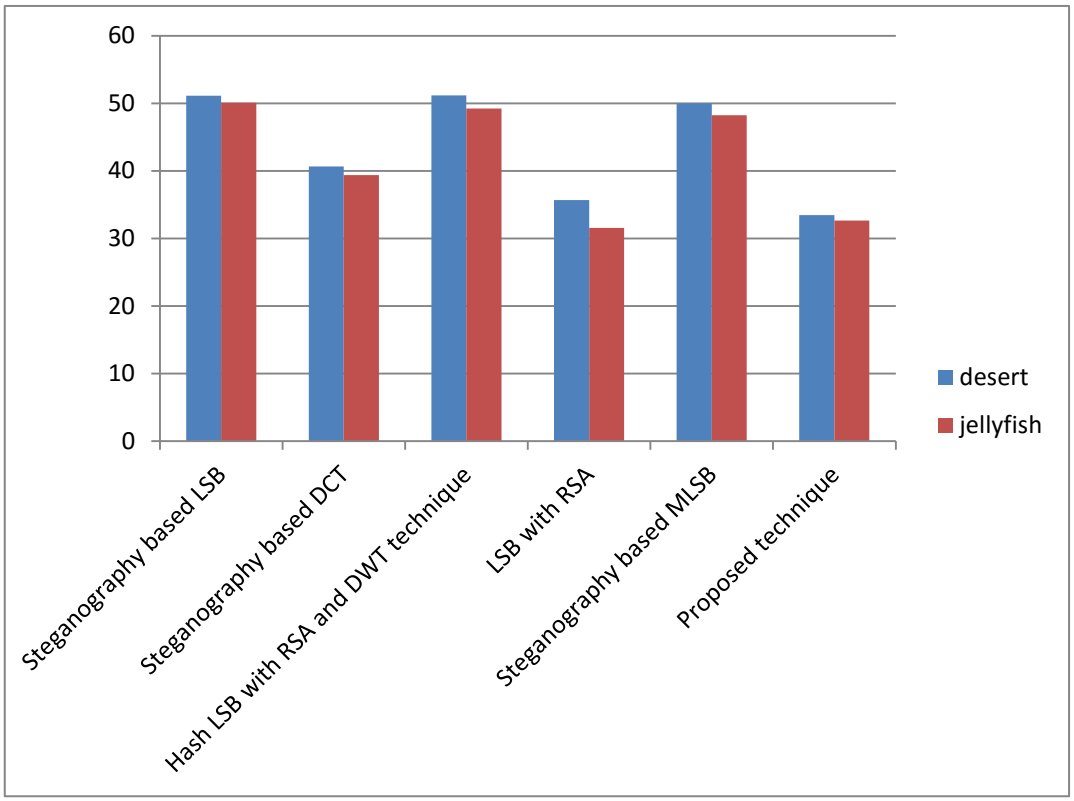
Decryption and Extraction



PSNR Values of Different Existing Techniques

Table 1: Comparisons to PSNR Values of Different Existing Techniques

METHODS	DESERT	JELLYFISH
Steganography Based LSB	51.10	50.10
Steganography Based DCT	40.67	39.39
Hash LSB with RSA and DWT Technique	51.18	49.24
LSB with RSA	35.67	31.54
Steganography Based MLSB	50.00	48.25
Proposed Technique	33.43	32.64

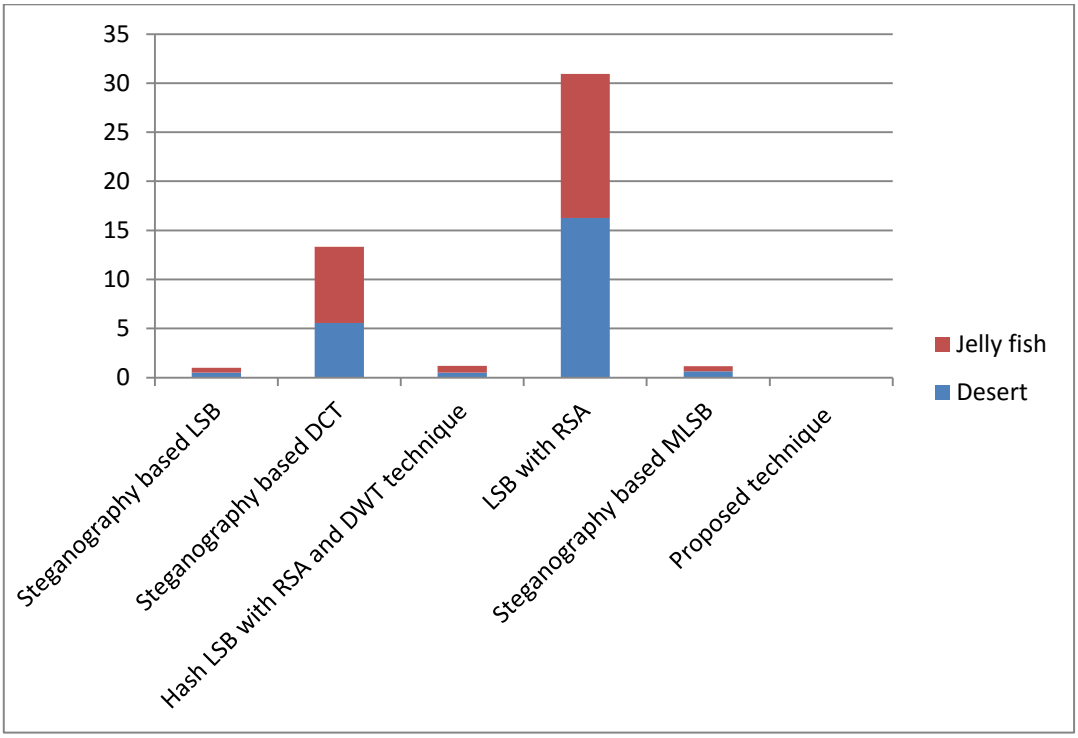


Comparisons Chart on PSNR Values of Different Existing Techniques

MSE Values of Different Existing Techniques

Table 2: Comparisons to MSE Values of Different Existing Techniques

Methods	Desert	Jelly fish
Steganography Based LSB	0.5035	0.4993
Steganography Based DCT	5.5684	7.7487
Hash LSB with RSA and DWT technique	0.4955	0.6987
LSB with RASH	16.2567	14.6743
Steganography Based MLSB	0.6228	0.5324
Proposed Technique	0.0089	0.0086



Comparisons Chart on MSE Values of Different Existing Techniques

V. CONCLUSION AND FUTURE WORK

In this age of universal electronic connectivity, of viruses and hackers, electronic eavesdropping and electronic fraud, there is a need to protect information from passing before curious eyes or, more importantly, from falling into wrong hands. Thus, multimedia security is much to consider in distributing digital information safety. Cryptography and Steganography are two important branches of information security. Cryptography provides encryption techniques for a secure communication. Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks. Steganography is the art and science of hiding communication .Steganography involves hiding information so that it appears as no information is hidden at all. Proposed approach enhances in more significant promotion in the terms of adaptability, capacity, and imperceptivity. Experimental results show that proposed approach obtains both larger capacity and high image quality with low errors. Finally we came to conclude that the proposed technique is effective for secret data communication. The future scope for the proposed method might be the development of a work by enhancing other data files like video, audio, image. Similarly the steganography technique can be developed for 3D images.

REFRENCES

[1] Nutan Manwade, Swati Nigam," LSB Image Steganography with DES Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015.

[2] Varsha, dr.Rajendar Singh Chhillar" Data Hiding Using Steganography and Cryptography," International Journal of Computer Science and Mobile Computing, vol.4, issue.4, April 2015.

[3] Ghania Al Sadi," Image Steganography Approach," International Journal Of Computer Science And Mobile Computing, Vol. 4, Issue. 8, August 2015.

[4] Blossom Kaur, Amandeep Kaur, Jasdeep Singh," Steganographic Approach for Hiding Image in DCT Domain,"July 2011.

[5] Ayushi, "A Symmetric Key Cryptography Algorithm," International Journal of Computer Applications, 2010.

[6] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.

[7] Priyanka Sahute, Swati Waghamare, Supriya Patil, Ashwini Diwate,"Secure Messaging Image Stegano graphy,"international Journal Of Modern Trends In Engineering And Research, 2015.

[8] A.M.Chandrashekar, Madhura S.Hegde, Aarabhi Putty," A Survey: Combined Impact of Cryptography and Steganography,"international Journal of Engineering Research Online, Vol.3, Issue 3, 2015.

[9] C. P. Shukla, R. S. Chadha, A. Kumar, "Enhance Security in Steganography with cryptography",International Journal of Advanced Research in Computer and Communication Engineering Vol. 3,Issue 3, March 2014.

[10] Wu D. C and Tsai W. H. (2003), "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626.