JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1162 - 1171
https://publishoa.com
ISSN: 1309-3452

Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms

Vikas Singhal
School of Computer Science & Applications
IFTM University,INDIA

Devendra Singh
School of Computer Science & Applications
IFTM University,INDIA

S. K. Gupta
BIET, Jhansi, INDIA

ABSTRACT

Evolving cloud has compelled people and organizations of every size – whether large or small to migrate data to public or private server for the reasons: scalability, agility, reliability, accessibility, cost saving. But along with the benefits, the risk to the safety of user data has also increased as it is always at a risk of data breach .Therefore, the Security and privacy of this data has become the most important foundation for a reliable server depository and a major challenge and key issue. We often ignore the safety of our data and completely rely on server service provider which is deficient .This paper proposes a crypto stegno technique using Blowfish and LSB (Least Significant Bit) algorithm for data encryption to secure sensitive data over the server from unauthorized access. Hence, preserving the privacy and securing the cloud stored sensitive data. The results are represented in the form of execution time, PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and the histogram of main and covered image. The experimental results reveal that all the algorithms achieve appropriate quality of stego image. They can be used as cryptographic algorithms to encrypt a message before applying steganography algorithms.

Keywords: Cryptography, Stegnography, DES, DCT, LSB, Blowfish

I. INTRODUCTION

Encryption is a well known technique for preserving the privacy of sensitive information but implementation of traditional encryption algorithm alone is not sufficient because with the enhanced data cyber attacks has also been evolved along with time. With increasing demand of information security, Encrypting and decrypting data has become an important research area and many techniques have been proposed, as it has a broad application prospect [1]. The recent ran some ware attacks show that cyber terrorism is becoming more and more common around the world. Therefore, it is more important now than ever to ensure the safety of sensitive data and that the organizations maintain compliance. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored over the server [2]. Government, military, financial institutions deals with geographical data for research, enemy positions (in defense, financial status. Most of this information is collected and stored on electronic devices and transmitted over network. If this information's fall into wrong hands then this breach can lead to declination of war.

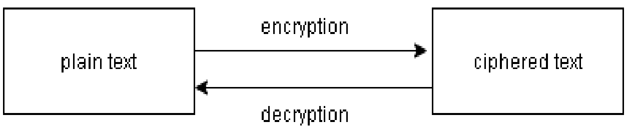


Figure.1: Encryption & Decryption Techniques

Therefore, often ignoring the risks associated with data storage along with the benefits and solely depending on cloud service providers for data safety is to consciously putting our data at risk [3]. This paper proposes a technique to add an extra layer of security to the data by implementing encryption at the level of data itself hence, securing the transmission as well as storage over the server. The proposed technique includes Blowfish algorithm which is a highly secured encryption algorithm due to its variable key size and LSB algorithm which widely used for stegnography, ensuring multiple security levels at the level of data itself [4].

II. BACKGROUND

Data encryption schemes have been increasingly studied over the period of time to meet the real time secure storage of data over the cloud many encryption algorithm have been proposed over a period of time to fulfill the demand of securing sensitive information over a network. Encryption is the process of encoding data into ciphered form that can only be read after proper decryption. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key to unscramble, or decrypt, the information. The development of cryptography has been paralleled by the development of crypt analysis, In 1993, Bruce Schneier designed a symmetric-key block cipher known as Blowfish [5]. It provides a good encryption rate in software. Blowfish has a 64-bit block size and a variable key length from 32 bits to up to 448 bits. It is a 16-round Feistel cipher and uses large key dependent S- boxes.LSB stegnography is a stegnography technique in which a message is hidden inside an image by replacing Least Significant Bit of image with the bits of message to be hidden. LSB is a widely used technique for image stegnography as it is much more reliable and secures [6]. In previous scenario, existing system is used as integration method which stores data by third party over cloud that has major concern to make confidentiality over cloud. For providing confidentiality for data in storage in any server, a user can encrypt the data by using cryptographic method before applying any other method to store and encode the data. When user wants to access the data for encrypting and decrypting, there is code be required for users from the server side by using cryptographic key. In general process there is limit of storage functionality for supporting some operations of encryption to data. In distributed architecture for storage systems offers better flexibility ans scalability, because server can be accessed and un accessed by any central authority [9].

III. PROPOSED METHODOLOGY

Our proposed technique provides the security of data in cloud storage by using encryption of data before uploading the data over the cloud minimum cost. To maintain the security of sensitive data, it can be better for encrypting the data before uploading over the server. The proposed method is implementation of Blowfish algorithm to encrypt only textual data buffering storing over the server and after that using a security key by using LSB algorithm with extra layer of security.

Proposed Algorithm's Steps:

The data transformation process for Pocket Brief uses the Blowfish Algorithm for Encryption and Decryption, respectively [10]. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneider as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. The actual encryption of data is very efficient on large micro processors [11]. Blowfish is a variable-length key block cipher. It is significantly faster than most encryption algorithms when implemented on 32-bitmicroprocessors with large data caches Feistel Networks

1.Login/Register
2.Choose an operation to perform-Encrypt/Decryption:

a. Encryption:

- check the box 'encrypt /decrypt to same folder' and 'delete plain file afterencryption'
- choose text file from desiredlocation.
- Click onopen.
- An encryption key is randomly generated from blowfish algorithm and provided to the encrypt or to enterand confirm the key to start the encryption process.
- Theencryption process of text file is initiatedusing blowfish algorithm and the key used using LSBtechnique
- .after encryption is finished click 'close 'and the encrypted file and the key is saved to the selecteddirectory.

b. Decryption:

- check the box 'encrypt/decryptto samefolder'
- chooseencrypted file from desired location
- Clickopen.
- enter encryptedkey used earlier to encrypt thesame text file for decryption .

- encrypted key is decrypted using LSB algorithm.
- enter and confirm the key for decription to decrypt the encryptedfile.
- after decryption is finished click on ‘close’ and the decrypted file is saved to the location.

c. Logout.

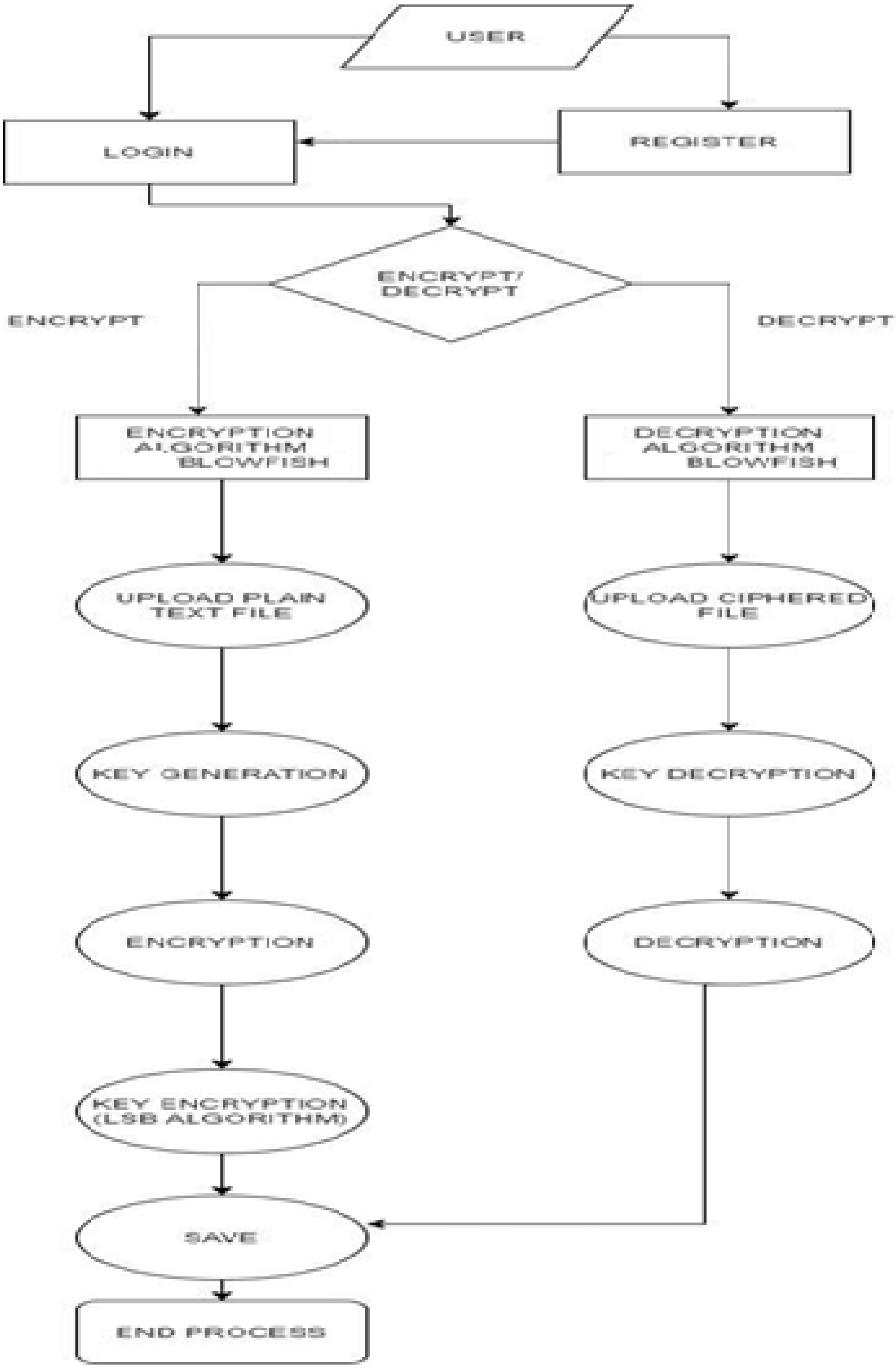


Figure.2: Flow Chart for Encryption and Decryption Techniques

IV. PROPOSED SYSTEM ARCHITECTURE

In our proposed system architecture we take the issue related to data security over the cloud. We presents use case diagram in figure.3 where key server and storage server are considered. Storing cryptographic key is a risky in a single device so, user can distribute cryptographic key subsequently for encrypting and decrypting the data which is finalized by cryptographic key for data security [12]. We proposes a new proxy re-encryption. The encryption key supports all the encoding operations over encrypted data and encoded data. In proposed architecture, user can access the encryption method for logging system and registration into the system so that user's uniqueness is tracked and maintained for encrypting and decrypting the data. The file can be stored for convenience of user. The user can settle for encrypting and decrypting which finalizes the action by generating encryption key to the end user for carrying out the procedure by using Blowfish algorithm and serves the encryption key by using LSB technique for accorded to the user and image steganography [13].

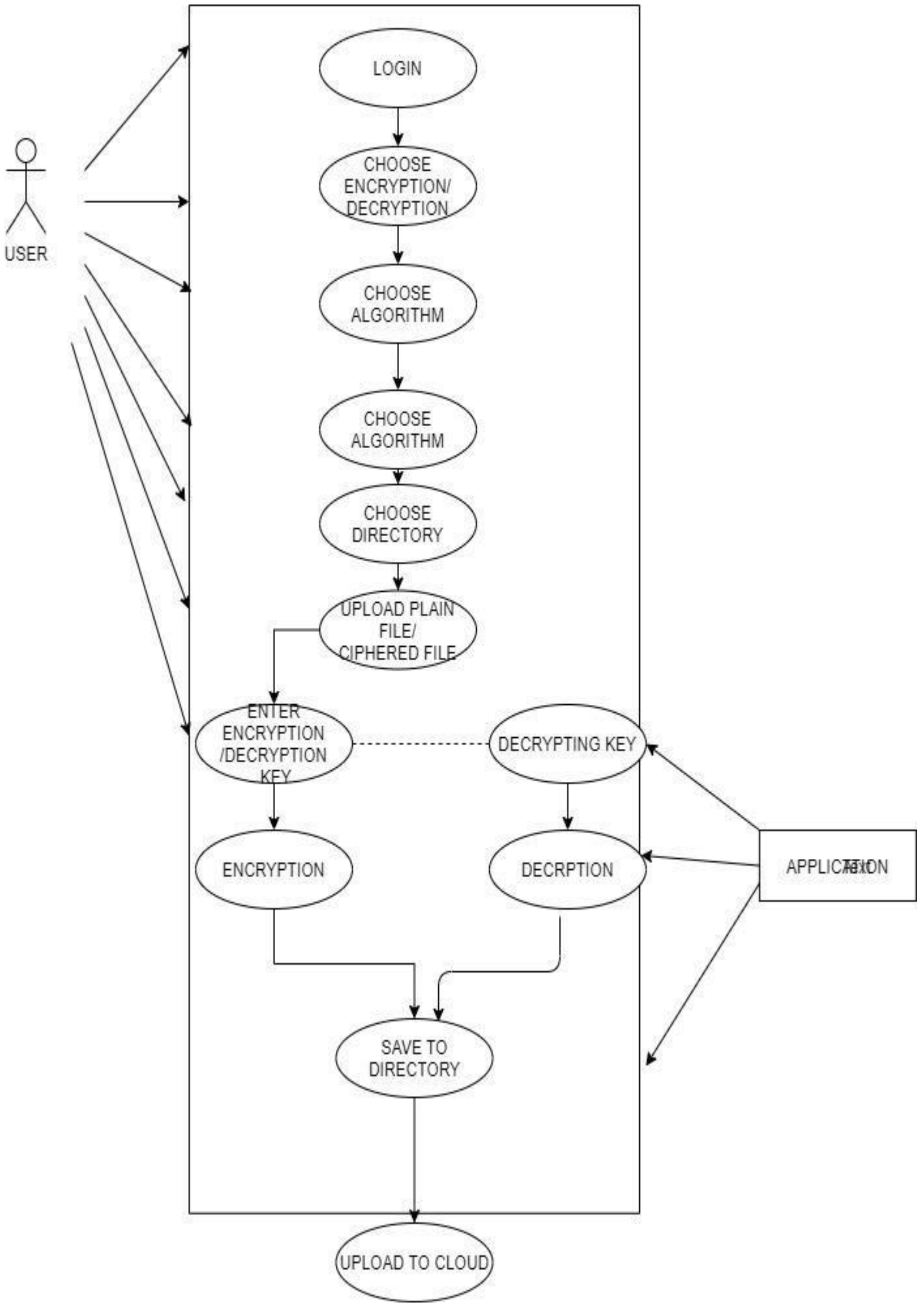


Figure.3: System Architecture for securing data over Cloud

The above architecture have following step for encrypting and decrypting the file over the cloud.

- Initially, the end user loggins'to the system.
- Following the successful login,the course of action is to be selected – ENCRYPTION/DECRYPTION.
- upload the textfile.
- the process is commenced by generating encryption key if chosen encryption or decrypting the encryption keyif chosen decryption.
- the text file is now encryptedor decrypted according to the operation selected to be performed.
- the new encrypted or decrypted file is now savedto the chosen directory.
- upload the text file tothe cloud.

V. IMPLEMENTATION AND RESULT ANALYSIS

In implementation, firstly we examine the created log file in the system with respect to time based on three parameters; authentication of user during the accessing of log file [14] and storage of data where we notice that our propose system architecture is better to store the data into the actual file over the cloud. For secure use of cloud the proposed technique is implemented as follows:

a. Successful login to the application which ensures accessibility for encryption using proposed technique. This maintains uniqueness of the user and authentication.

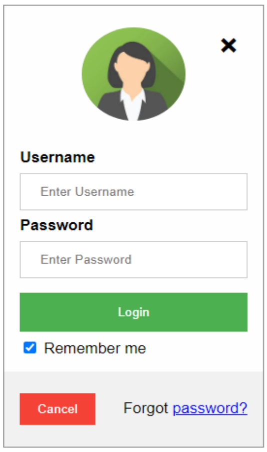


Figure. 4:System login for encryption

b.Following the above process, the user needs to choose whether to encrypt or decrypt the file.

c. an encryption key is generated of variable size 32-448 bits using Blowfish encryption algorithm , which divides the message into fixed length blocks of 64 bits during its process and performes encryption for 16 rounds which is prone to attack till date.And the text file is encrypted and ready for server offloading.

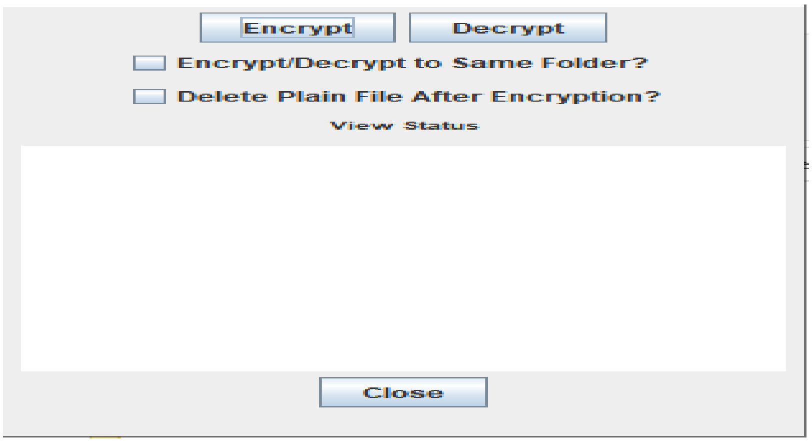

Encrypt
Decrypt
□ Encrypt/Decrypt to Same Folder?
□ Delete Plain File After Encryption?
View Status
Close

Figure.5. System encrypt/decrypt for text file

d.After the encryption process ends , the encryption key is itself encrypted using LSB encryption algorithm for image stegnography which encrypts the key into a cover image for a secure storage and a new encryption key is generated for this .

e. For decrypting the same text file ,the encryption key is first decrypted i.e., recovered from the cover image using LSB encryption key. Finally, the encrypted file is decrypted using the recovered encryption key.

VI. Comparison of Existing and Proposed Algorithm

Blowfish algorithm is much better than other existing method for creating encyption key. In the given table.1 we can see the comparison of implemented Blowfish algorithm has better from other symmetric algorithms. Hence, the proposed technique is implementation of Blowfish algorithm that is much more secure as it uses blowfish algorithm and also LSB algorithm for image stegnography to secure the encryption key itself providing multilayer protection to the user data.

Table.I. Comparison of Symmetric Algorithm

S.no.	**Algorithms**	**Key size**	**Block size**	**round**	**structure**	**flexible**	**features**
1	DES	64 bits	64 bits	16	Feistel	No	Not structure, enough
2	DCT	112 or 118 bits	64 bits	48	Feistel	Yes	Adequate security
6	BLOWFISH	32-448 bits	64 bits	16	Feistel	yes	Excellent security

We have also taken the images, those are considered to be 512×512 pixels. The message which is considered to be encrypted with the five mentioned algorithm is around 1Kbits. The plaintext is the same for all five cryptographic algorithms. The first comparison is based on encryption time including key generation which is depicted in Table I. These implementations are on MATLAB (R2016a) which import java programs of five algorithms. The implementations of five algorithms are performed on the same environment [15].

Fig. 1. (a) Peppers (b)Baboon cover images

The key length for each algorithm is considered as the most common key length that are still secure and employed in applications. The results represent that the worst encryption time including key generation is for RSA cryptographic algorithm. It is a public key algorithm and needs two key for operation. In the following, the time of decryption of algorithms are shown in Table II.

Table II. Decryption time of DES, DCT, and Blowfish

Algorithm	Key length bits	Decryption time seconds(s)
DES	56	0.000750
DCT	168	0.001046
Blowfish	128	0.000866

The decryption time is less than encryption time due to the key generation is not considered in these times. The other quality metrics used to evaluate the steganography employing the five cryptographic algorithms and the LSB technique are the signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR) and Mean Square Error (MSE). PSNR value defines the image quality. The more the PSNR value is, the higher quality the image has. The PSNR value should not be less than 30dB in decibels [15]. MSE indicates the degree of differences or similarity between original image and steganography image. The less the MSE value of an image is, the better the quality and distortion from the original is [16].

$$MSE = \frac{\sum_{M,N}\left(T(r,c) - T'(r,c)\right)^2}{M*N}$$

(1)

Where, M is the total number of rows, N is total number of columns, (r,c) are rows and columns respectively, T is original image T' is the changed image.

Peak Signal to Noise Ratio (PSNR) is the ratio between maximum possible power and corrupting noise that corrupts the representation of the image. Higher is the value, better is the quality of the image [17].

(2) $$PSNR = 10*\log_{10}\left[\frac{R^2}{MSE}\right]$$

R is the maximum fluctuation in the input image data type. Table III depicted The SNR, PSNR and MSE values of AES, RSA, DES, 3DES and Blowfish algorithms and peppers image as the cover image.

Table III. Encryption time of DES, DCT, and Blowfish

Algorithm	Key length bits	Encryption time seconds(s)
DES	56	0.004064
DCT	168	0.004734
Blowfish	128	0.004357

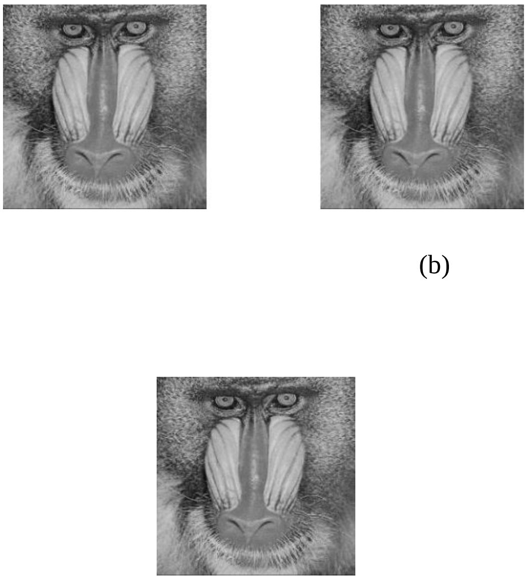
Table IV. The SNR, PSNR and MSE values of AES, RSA, DES, 3DES,(b)and Blowfish and Peppers as cover image

Algorithm	SNR	PSNR	MSE
DES	66.6623	72.3989	0.0048
DCT	66.5623	72.2989	0.0038
Blowfish	66.4455	72.1920	0.0037

Table V. The SNR, PSNR and MSE values of AES, RSA, DES, 3DES, and Blowfish and Baboon as cover image

Algorithm	SNR	PSNR	MSE
DES	66.6753	72.1132	0.0039
DCT	66.5870	72.2249	0.0038
Blowfish	67.0365	72.3845	0.0037

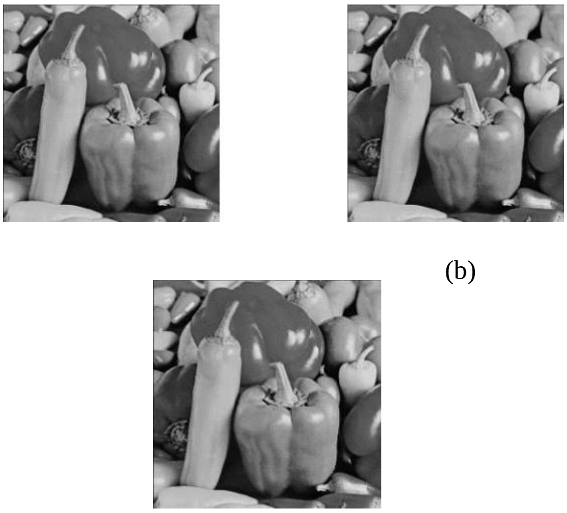
The best results are obtained by high PSNR and less MSE. Table IV depicted The SNR, PSNR and MSE values of DES, DCT, and Blowfish algorithms and Baboon image as the cover image. The results using of DES, DCT and Blowfish algorithms as cryptographic algorithms and LSB as steganography algorithm using Peppers and Baboon images as cover images illustrates perfect values. The Stego images of using Peppers and Baboon are shown in Fig. 2 and Fig. 3 respectively.



(a) (b)

(c)

Fig. 2 Stego images of employing (a) DES (b) DCT (c) Blowfish and Peppers as cover image

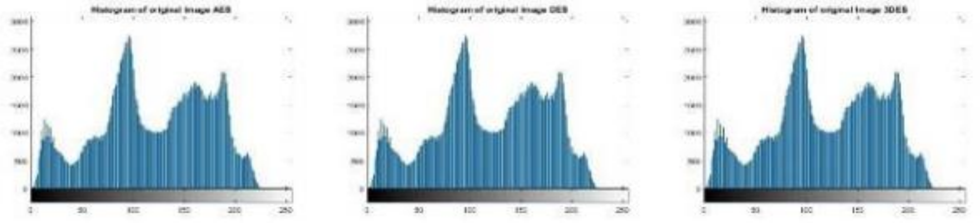


(a) (b)

(c)

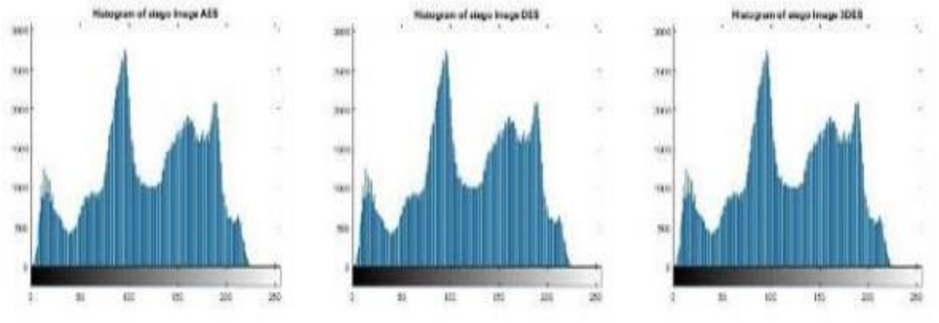
Fig. 3 Stego images of employing (a) DES (b) DCT (d) Blowfish

Fig. 1 shows the input cover images of size 512 × 512 whereas Fig. 2 and Fig. 3 illustrates the resulting stego images employing DES, DCT, and Blowfish algorithms. Histogram analysis between the cover image and stego image are illustrated to measure robustness against common statistical attacks [18]. The histogram of stego images and the histogram of cover image are compared in Fig. 4 and Fig. 5. The analysis results represent that there is no significant difference in histograms of the cover and stego images.



(a) (b) (c)

Fig. 4 Histogram of Peppers cover image employing (a) DES (b) DCT (c) Blowfish



(a) (b) (c)

Fig. 5 Histogram of Peppers stego image employing (a) DES (b) DCT (c) Blowfish

VII. CONCLUSION

The proposed technique ensures more security to user data over the server providing multilayer protection to the user as even if the data falls into wrong hands it is useless as long as its key remain secure. This way it protects data contents in the event that a provider, account, system is compromised. This proposed technique is aimed to encrypt /decrypt text data before storing on the server which is cost efficient. But in future, this technique can be enhanced to encrypt all types of data including audio, video and image cryptography. In this paper, cryptography and steganography are combined to achieve higher security. The cryptographic algorithms are DES, DCT and Blowfish algorithms and the steganography technique is LSB. First, the data is encrypted via the mentioned algorithms. Then the secret message is embedded into the LSB algorithm to be hidden in a cover image. The experimental outcome of the method is performed on MATLAB. Two error metrics are employed to compare the quality of cover image and the stego image. The high PSNR and low MSE represent the satisfaction of employing these algorithms for the first step of the method. The encrypted message is also not easily detected by the difference histogram analysis while employing cryptographic algorithms for the first step of steganography.

REFERENCES

[1] V.Harikrishna, A. Rama, N.Deeepa, A secure file storage in Cloud Computing using Hybrid Cryptography, TEST Engineering & Management, vol 82, Feb 2020

[2] S.V.N. Srivavalli, Ben Swarup Medikonda, Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography, International Journal of Recent Technology and Engineering, vol.8, issue 1, May 2019

[3] Chungsik Song, Younghee Park, Jerry Gao, Sri Kinnera Nandun, William Zegers, Favored Encryption Techniques for Cloud Storage, The First IEEE International Conference on Big Data Computing Service and Applications, California, USA 2015

[4] Masumeh Damrudi, Kamal Jadidy Aval, Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES and Blowfish, International Journal of Engineering and Advanced Technology, vol.8, issue 6S3, Sept 2019

[5] Bruce Schneier, Applied Cryptography Protocols, Algorithms and Source Code in C, John Wiley & Sons, ISBN 978-1-1119-096726, 1996

[6] Mohmmad Obaidur Rahman, Muhammad Kamal Hossen, Golam Morsad, Animesh Chandra Roy and Shahnur Azad Chowdhury, An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique, vol.18, issue 9, Sept 2018

[7] K.R. Sajay, Suvanam Sasidhar Babu & Yellepeddi Vijayalakshmi, Enhancing the security of cloud data using hybrid encryption algorithm, Journal of Ambient Intelligence and Humanized Computing, 2019

[8] Gunavathy, Meena, A Survey: Data Security in Cloud using Cryptography and Steganography, International Research Journal of Engineering and Technology, vol.06, issue 05, May 2019

[9] Abdullah TH Abdalsatiri, Mohd. Farooq Hamdi, Ali Noori Kareem, Data Security in Cloud by using Blowfish Algorithm, International Journal of Scientific Engineering and Technology Research, vol.03, issue 01, January 2014, pp 0158-0162

[10] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, Steganography in Images Using LSB Technique, International Journal of Latest Trends in Engineering and Technology (IJLTET), vol.5, issue 1, January 2015 ISSN: 2278-621X

[11] D.coppersmith,"The Data Encryption Standard(DES) and its strength Against Attacks., IBM Journal of research And Development, pp 243-250, May 1994

[12] A Nadeem and M.Y. Javed, A Performance Comarison of Data Encryption Algorithms, IEEE International Conference on Information and Communication Technologies, Karachi, Pakistan, pp 84-89, February,2005

[13] P.Princy, A Comparison of Symmetric Key Algorithms DES, AES, Blowfish, RC4, RC6: A Survey, International Journal of Computer Science & Engineering Technology, vol.6, issue05, May 2015

[14] Hemlata Sharma, Dinesh Goyal, Security of Data within Video using Steganography & Crptography, International Journal of Trend in Research and Developement, vol3, issue 4, Jul-Aug 2016

[15] A. Pandey, and J. Chopra, "Steganography using AES and LSB techniques", International Journal of Scientific Research Engineering & Technology (IJSRET), vol. 6, no. 6, 2017, pp. 620-623.

[16] A. Pandey, and P. Bonde, "Performance evaluation of various cryptography algorithms along with LSB substitution technique", International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 6, 2013, pp. 866-871.

[17] S. Nagpal, and R. Nagpal, "Collaboration of cryptography and steganography for enhanced security: a review", International Journal of Innovative Knowledge Concepts, vol. 6, no. 8, 2018, pp. 124-128.

[18] The USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 6 July 2019).