ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Efficient Data Security by combination of Cryptography and Steganography

Puja[1], Dr. Dinesh Kumar[2]

P.G. Student, Department of Computer Engineering, Shri Ram College of Engineering and Management, Palwal, Haryana, India[1]

Associate Professor, Department of Computer Engineering, Shri Ram College of Engineering and Management, Palwal, Haryana, India[2]

ABSTRACT: As utilization of PC systems and web is becoming quick and appreciating step by step, data security is turned into a noteworthy worry in PC systems. There is dependably chance infringing upon organize security which drives a need of a productive and basic method for securing the electronic reports from being perused or utilized by individuals other than who are approved to do it. Encryption is one of the security strategy generally used to guarantee mystery. Encryption is a totally scientific process that takes in information, plays out some predefined numerical tasks on the information, and after that yields the outcome. Blowfish is one of the superlative encryption calculations since it requires less execution time, memory and has high throughput. Be that as it may assuming any meddler recognizes the nearness of encoded information he or she can attempt a few assaults so as to get the first information. So there is a need to give a two layer way to deal with better security. That is the reason this work shows a security framework utilizing blend of cryptography and steganography to upgrade the security.

KEYWORDS: Cryptography, Steganography, Security, Encryption, Decryption, Blowfish.

I. Introduction

Cryptography and Steganography are surely understood and generally utilized systems that control data (messages) keeping in mind the end goal to figure or conceal their reality separately. Steganography is the workmanship and investigation of imparting in a way which conceals the presence of the correspondence. Cryptography scrambles a message so it can't be comprehended; the Steganography shrouds the message so it can't be seen. In this paper we will center to create one framework, which employments both cryptography and Steganography for better classification and security. By and by we have extremely secure strategies for both cryptography and Steganography - AES calculation is an extremely secure strategy for cryptography and the Steganography techniques, which utilize recurrence area, are profoundly secured. Regardless of whether we consolidate these systems straight forwardly, quite possibly the gatecrasher may recognize the first message. Consequently, our thought is to apply them two together with greater security levels and to get a highly secured framework for information covering up.

This paper predominantly centers around to build up another framework with additional security highlights where a significant bit of instant message can be covered up by consolidating security strategies likeCryptography and Steganography. Steganography is an innovation that installs a private message or picture inside content, or a computerized picture or advanced recordings or advanced sounds. It is at some point mistook for cryptography, not in name however, in the utilization. The straightforward method to separate that steganography hides not just the substance of the message yet additionally the minor presence of a message from a spectator so there is no odds of uncertainty of the presence of the message, where as in cryptography the reason for existing is to secure correspondence from programmers by changing over secret message into not reasonable shape. It is seen from past encounter that sending encoded data may make doubt while undetectable data won't do as such.

DOI: 10.15680/IJIRCCE.2018.0605027

II. Related work

In [3] a steganographic scheme was proposed, it uses human vision sensitivity to hide secret bits. To make this, the secret data firstly are converted into a series of symbols to be embedded in a notation system with multiple bases. In this case, the particular bases used are determined by the degree of local variation of the pixel magnitudes in the host image. A modification to the least significant bit matching (LSBM) steganography was introduced in [4].DWT based frequency domain steganographic technique was proposed in [9], the data is hidden in horizontal, vertical and diagonal components of the sub – image. In [10] a secret data communication system was presented, it employs RSA with asymmetric keys and AES with symmetric key to encrypt the data, after that the encrypted data is embedded into the cover image using smart LSB pixel mapping and data rearrangement method. In [11] and [12] two secure communication systems were proposed to be used for voice over IP (VOIP) applications.

III. Proposed Method

In a summarized way it could be concluded that SQL becomes the query engine that resides over the database engine having been designed on the client-server Approach and provided retrieval of data as well as operation on RDBMS. By the Application package and web pages.

1. Data Flow Diagram

Data flow diagrams illustrate how data is processed by a system in terms of inputs and outputs. Data flow diagrams can be used to provide a clear representation of any business function. The technique starts with an overall picture of the business and continues by analyzing each of the functional areas of interest.

DataFlow Diagram : (Level-0) :

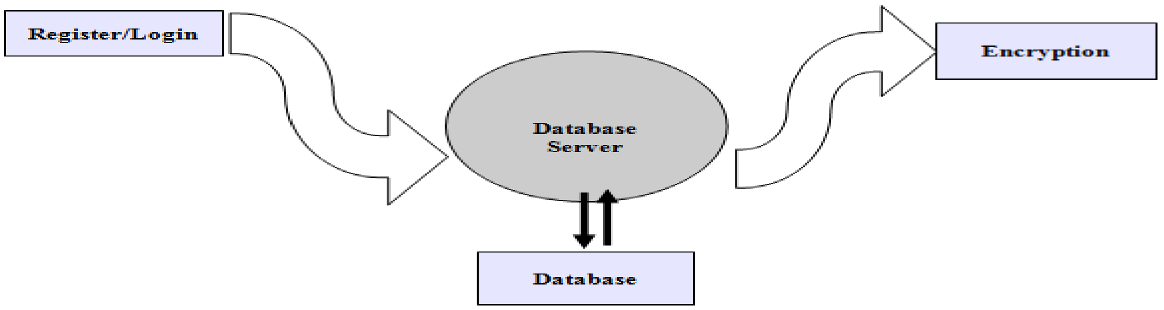


Fig 1. Level 0 DFD

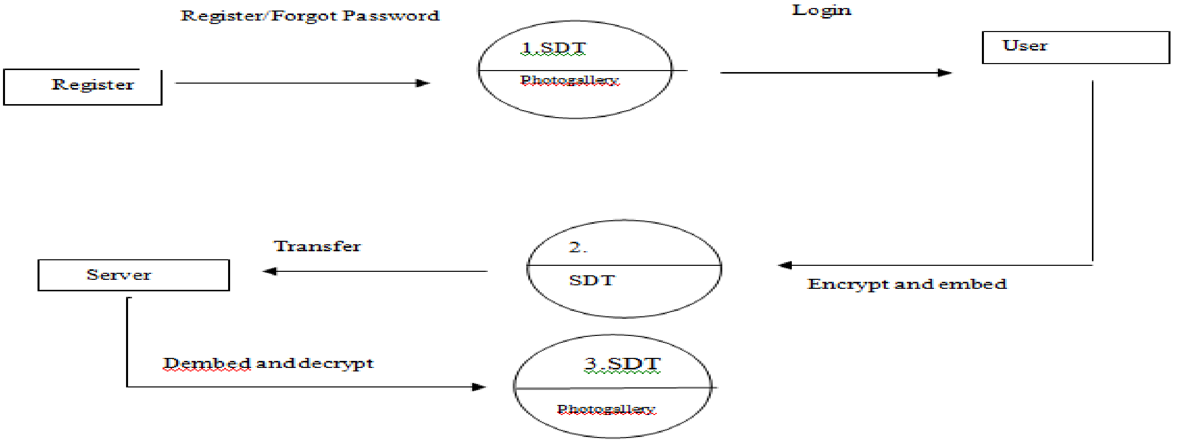


Fig. 2 Level – 1 & 2 DFD

II. CRYPTOGRAPHIC ALGORITHM

2.1 Blowfish

Blowfish is a Feistel network block cipher with a 64 bit block size and a variable key size up to 448 bits long. The Blowfish algorithm is unencumbered by patents and is free to use for any one is any situation. Blowfish consists of two parts: key-expansion and data encryption.

2.2 AES

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys.

2.3 DES

The DES calculation in light of LUCIFER, outlined by Horst Feistel, was created at IBM in 1972. This calculation was endorsed by the National Bureau of Standards (now NIST) after evaluation of DES quality and changes by the National Security Agency (NSA), and turned into a Federal standard in 1977.

2. STEGANOGRAPHY

3.1 Least Signifcant Bit (Lsb)

LSB is the most reduced piece in a progression of numbers in double. e.g. in the double number: 10110001, the minimum huge piece is far right 1. The LSB based Steganography is one of the steganographic techniques, used to insert the mystery information in to the minimum huge bits of the pixel esteems in a cover picture.

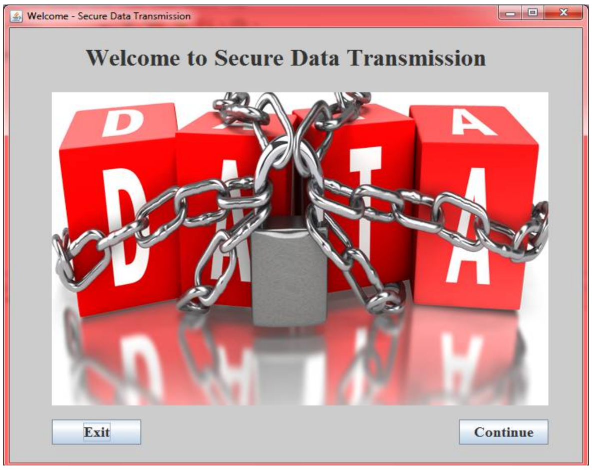
a. Discrete Cosine Transform (Dct)

DCT coefficients are utilized for JPEG pressure. It isolates the picture into parts of varying significance. It changes a flag or picture from the spatial area to the recurrence space. It can isolate the picture into high, center and low recurrence segments.

IV. SIMULATION RESULTS

The simulation studies involve the process of secure data transmission. Fig. 1 indicate Welcome Page, here is the option to continue to the register page. Fig.2 indicate registration form. Fig.3 indicate login form. Fig. 4 indicate home page there is the option to encrypt, decrypt, embed, deembed the data. Fig 5. indicate encryption process. Fig 6. indicate

Decryption process. Fig 7 indicate embedding process Fig 8. indicate deembedding process. Fig. 9 indicate to select the secure data and send it to receiver location. Fig 10. indicate the graph analysis of all algorithm used in Cryptography.


Welcome - Secure Data Transmission

Welcome to Secure Data Transmission

Fig. 1 Welcome Page

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

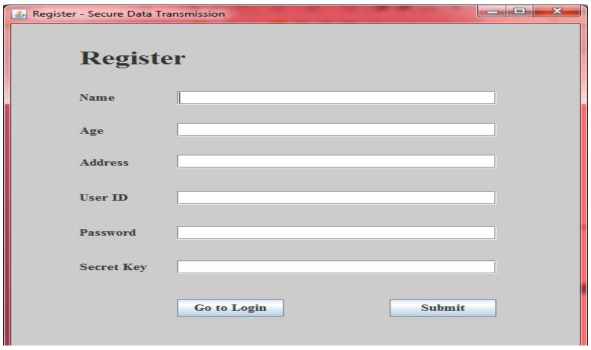


Fig. 2 Registration Form

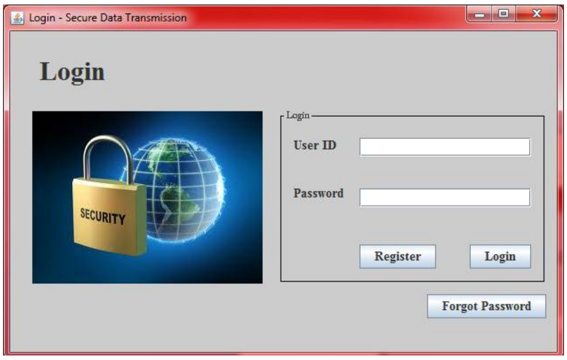


Fig. 3Login

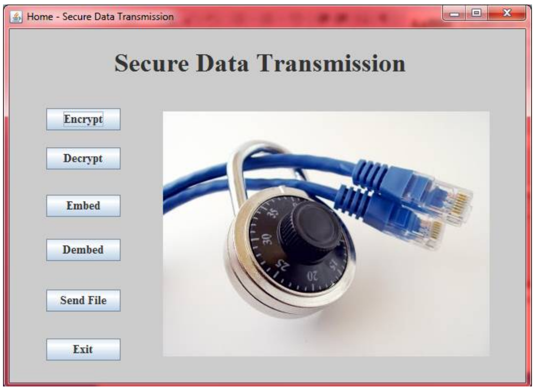
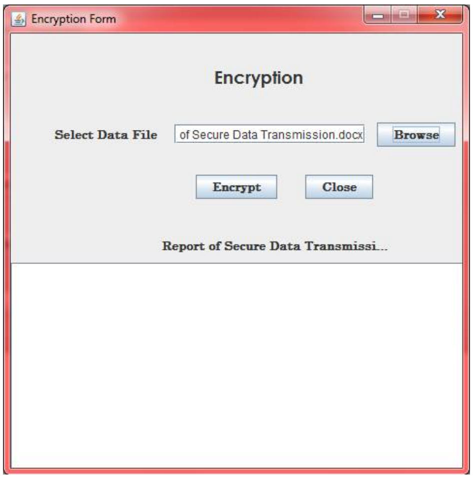


Fig.4Home Page

DOI: 10.15680/IJIRCCE.2018.0605027



Select Data File: of Secure Data Transmission.docx

Report of Secure Data Transmissi...

Fig. 5Encryption

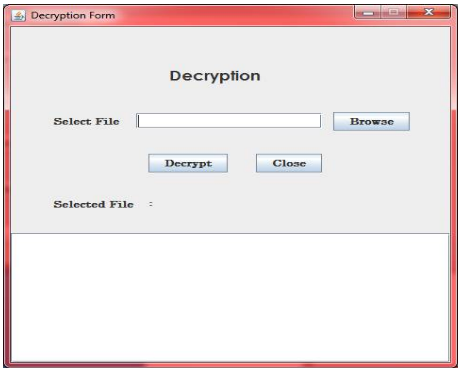


Fig. 6Decryption

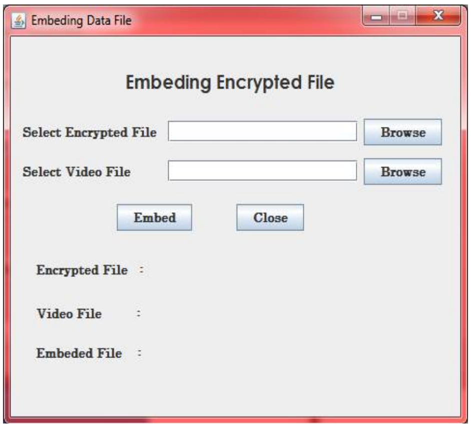


Fig. 7Embedding

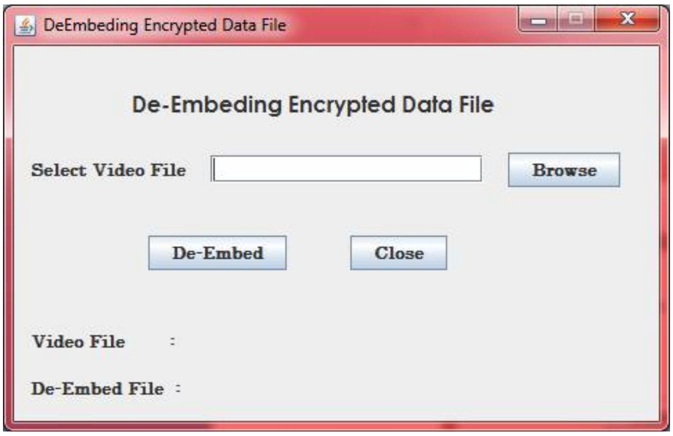


Fig. 8De-Embedding

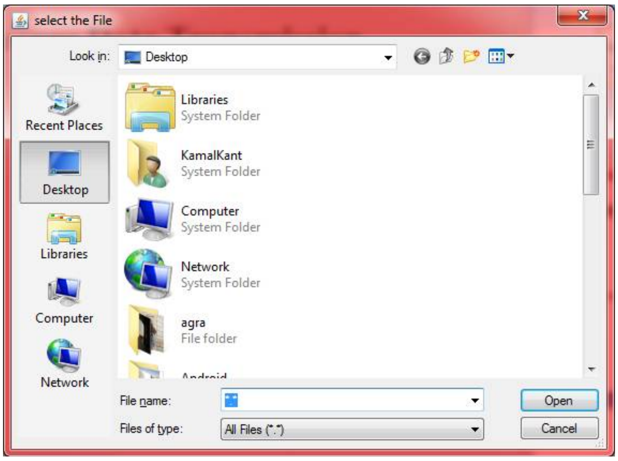


Fig. 9Select a file for sending

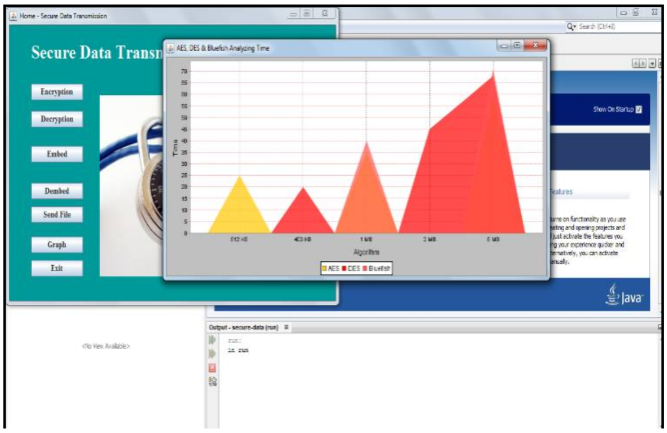


Fig. 10Graph Analysis

V. CONCLUSION AND FUTURE WORK

To make the information secure from different assaults and for the uprightness of information, we should scramble the information before it is transmitted or put away. So in this work blowfish calculation alongside steganography is executed to secure delicate information by making hard to recognize the nearness of concealed message. Two layer approach of security is executed and a few conclusions are made as recorded beneath.

- Blowfish calculation is one of the superlative encryption calculations since it requires less execution time, memory and has high throughput.
- In this paper we have exhibited another framework for the mix of Compression, cryptography what's more, Steganography utilizing three keys which could be demonstrated a very secured strategy for information correspondence in not so distant future.
- In the future work, we are looking forward to try applying the proposed method on audio and video.

REFERENCES

1. Obaida Mohammad Awad Al-Hazaimeh, "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, 2013
2. Katzenbeisser, S. and Petitcola, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London, 2000.
3. Xinpeng Zhang and Shuozhong Wang, "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1, 2005.
4. Jarno Mielikainen, "LSB Matching Revisited", IEEE signal processing letters, Vol. 13, No. 5, 2006.
5. Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1, pp. 127- 134, 2010 .
6. D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210
7. Mamta Sharma, S.L. Bawa D.A.V. college: Compression Using Huffman Coding, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010
8. Kharrazi, M., Sencar, H. T., and Memon, N, Image Steganography: Concepts and practice. In WSPC Lecture Notes Series, Vol.5, No.3, 2004
9. DAVID A. HUFFMAN+, ASSOCIATE, A Method for the Construction of MinimumRedundancy Codes, PROCEEDINGS OF THE IRE.
10. Daemen, Joan; Rijmen, Vincent. AES Proposal: Rijndael. ijndael.pdf
11. Provos, N. and Honeyman, P. Hide and seek: An introduction to steganography. IEEE SECURITY & PRIVACY, 2003
12. Owens, M., “A discussion of covert channels and steganography”, SANS Institute, 2002