International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Automatic User Legitimacy Verification on Cloud Health Care Networks

Gagandeep Kaur[1], Gurbinder Singh Brar[2]

[1]*Research Scholar*

[2]*Associate Professor, AIET, Faridkot*

ABSTRACT

The secure data storage on cloud environments is the primary requirement of such applications, where data are being transferred or transmitted between the servers and their users. The data security is quite important because they belongs the users. With an internet based development and use of computer technology several trends are opening up in the era of cloud computing. Moving data into the cloud offers much ease to users since they don't have to care about the complexities of managing hardware directly. Steganography is the practice of hiding a content of a file. a message, image, or video within other file, message, image, or video. Generally, the hidden messages appear to be part of other: images, articles, shopping lists, or some other cover text.

Keywords: Cover Image, LSB, CIBE, Encryption, Compression, Blurring

I. INTRODUCTION

The secure data storage on cloud environments is the primary requirement of such applications, where data are being transferred or transmitted between the servers and their users. The data security is quite important because they belongs the users. With an internet based development and use of computer technology several trends are opening up in the era of cloud computing.

Moving data into the cloud offers much ease to users since they don't have to care about the

complexities of managing hardware directly. The explorer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Cloud Compute(EC2) both are well known examples .These internet-based online services do provide huge amounts of storage space and customized computing resources, computing platform shift, however, is reducing the responsibility of local machines for maintaining data at the same time. As a result, for the availability and integrity of their own data users area the mercy of their cloud service providers.

Cloud Computing naturally raises new challenging security threats for many reasons. First, traditional cryptographic basics for protection of data security cannot be directly adhered due to the loss control of data by users under Cloud Computing. Therefore, verifying the storage of correct data in the cloud must be performed without clear knowledge of the whole data. Considering different data for every user stored in the cloud and the demand of continuous data security as security, the problem of verifying correctness of data

storage in cloud becomes even more challenging. Secondly, Cloud Computing is not a data warehouse by third party. The stored data in the cloud may be frequently updated by the users, which include deletion, insertion, appending, modifying, reordering, etc. To ensure correctness of storage for updation of dynamic data is of much importance. Last button the least, the evolution of Cloud Computing is done by data centers running simultaneously with co-operation and in distributed manner.

Since users are focusing on single server scenario and most of them do not consider data operations performed dynamically, the techniques, which can be useful to ensure the correctness of storage without having users possessing data, cannot address all the cloud data storage security threats. So researchers have proposed distributed protocols for ensuring storage correctness across different servers as an complementary approach. Steganography is the practice of hiding a content of a file ,a message, image, or video within other file, message, image, or video. The word steganography is a combination of Greek words steganos, means "covered" and 'graphie' means "writing".

The recorded first use of the term was in 1499 by Johannes Trithemius in his Steganographia, a study on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be part of other: images, articles, shopping lists, or some other cover text. For example, the message i.e hidden may be in form of invisible ink between the visible lines of a private letter. Some implementations of steganography in the forms of security through obscurity that lack a shared secret, whereas key-dependent steganography schemes implements Kerckhoffs's principle. The benefit of steganography over cryptography alone is that the original secret message does not attract attention to itself as an object of close examination. Thus, whereas cryptography is the practice of securing only the message contents , steganography is concerned with concealing the fact of sending a secret message , as well as protecting the contents of the message. When steganography is combined with encryption it provides high level for security Encryption deals with converting the plain text into cipher text.

II. LITERATURE SURVEY

Prof. Christopher, "APPLIED CRYPTOGRAPHY AND DATA SECURITY" [12]. Thesis an article written by Prof Christopher on the all popular applied cryptography and data security. The author has discussed all popular encryption algorithms with their advantages and disadvantages along with the detail of algorithmic structure of the algorithm.

Gary C. Kessler, "An Overview of Cryptography". It is an old paper based on cryptography by Gary C. Kessler, and since then till date it was continuously updated . It was last updated in 2014. The author suggested again the great source for the cryptography algorithms. Before putting it in the use it is very important to understand the structure of the encryption algorithm

Milind Mathur *et al.*"Comparison between 3DES, DES, RC2 , RC6, BLOWFISH AND AES". The authors have examine the encryption algorithms. The detailed survey on encryption algorithms covers all of the popular and prominent algorithms. This survey shows that blowfish is the best encryption algorithm and outperformed all others. Blowfish takes least time and provides maximum throughput.

Verma O.P., Agarwal R., Dafouti D., "Performance analysis of data encryption algorithms", In this research,it have presented two main characteristics that identify and differentiate one encryption algorithm from other is its ability to protect the data against attacks and its speed and efficiency in doing so. This paper provides a comparison based on performance between most common encryption algorithms: DES, 3DES, Blowfish and AES . The comparison was conducted by running several encryption settings to evaluate the algorithm's encryption/decryption speed by processing different sizes of data blocks.

Mamta Juneja and Parvinder S. Sandhu ,"An Steganography Technique based on LSB for RGB Color Images" In this paper for stegnography least significant bit(LSB) technique is used which provides better security .It helps in hiding the encrypted data in pixel location that is adjacent and random in locations in edges .It detects edges in the cover image, then message bits are embedded in randomly selected edge area pixels with the least significant byte. It ensures that the attackers will not have any knowledge that message bits are hidden in the image .

III. PROBLEM DEFINITION

In this day and age, body sensors are being utilized at a huge to screen the patients in their standard movement post-or pre-treatment. Wearable body sensors more often than not sends information to the medicinal databases straightforwardly through the remote mediums (cell systems, Wi-Fi, Zigbee, and so forth.). The patients are educated by the restorative database fixates about their wellbeing on week by week or month to month premise by sending reports to their home or on their messages. The social insurance checking information is totaled on the servers and different kinds of calculations are

utilized for the medicinal services information investigation. The client security turns into the significant worry in such medicinal services checking frameworks. The validation plot based social insurance information protection calculation in the base paper has been proposed. The current validation plot depends on secure key trade. In this exploration, we are attempting to take care of the issue of secrecy and information honesty by including different security conventions and calculations with the current verification in view of social insurance checking frameworks.

IV. PROPOSED MODEL

In this paper proposed model for client information security in medicinal services observing framework will be a blend of information pressure, encryption and verification plans. The new half breed client protection model will guarantee the security level solidifying for the safe information moves in the human services observing frameworks. The classification of the client sending the information will be accomplished by utilizing the protected key trade between the medicinal services sensors and therapeutic database. The protected key trade model will be refresh in the proposed demonstrate than the current client security arrangement in the base paper. The key table for proposed plan will utilize randomized numerical key age capacities. The key table sharing will be performed in the neighbor building condition of the security demonstrate. To go up against the information honesty, the encryption calculation will be utilized. The encryption calculation will guarantee the protection of

the client information by making the information mixed up amid information transmissions between the medicinal databases and social insurance sensors.

V. EXPERIMENTAL DESIGN

The design of the proposed image security framework works in three phases i.e. image compression, image encryption and blurring. In the first phase, the image (hidden object) is compressed to reduce its size. The size is reduced to facilitate smooth internet transfers as well as less memory enhancement during blurring and encryption algorithms. The second phase is image encryption. The compressed image is encrypted to add another security layer, which hardens the image security. The phase consists of blur map based blurring algorithm, where the image is converted to secret blur image. The flow diagram of the proposed digital blurring and encryption algorithm is presented in the Figure 5.1.

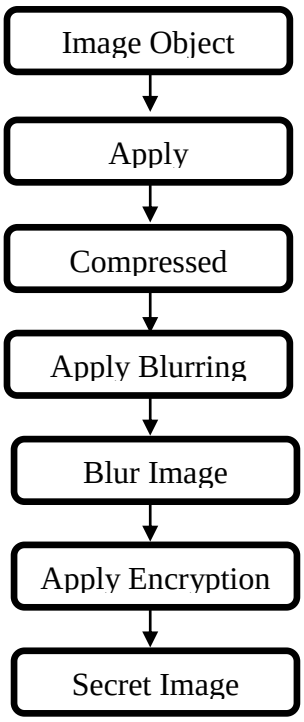

Figure5.1: Design of proposed algorithm

Algorithm: Compress Method

1. The image is broken in smaller parts, say 8x8 pixels
2. Working from left to right, top to bottom, the DWT is applied to each block
3. Each block is compressed through quantization
4. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.

5. When desired, the image is reconstructed through decompression, a process that uses the inverse discrete wavelet transform (iDWT).

Key Generation Policy: Key generation policy in the designed model uses following algorithm and mathematic formula to generate random keys and then stored in key table. This key table is stored in workspace and being exchanged between nodes.

Algorithm: The proposed Encryption Process

1. Input Image
2. Convert the image into Data Matrix (d)
3. Data Matrix Validation →validate(d) →d_M
4. Data Matrix Segmentation →segment((d_M) →d_m^i
5. Input Security Key (S_k)
6. Key Expansion(S_k)
7. Initial Round→Add Round Key (S_k)
8. Rounds → For Loop
    a. *Sub Bytes(d_m^i)*
    b. *Shift Rows(d_m^i)*
    c. *Mix Columns(d_m^i)*
    d. *Add Round Key(d_m^i)*
9. Rounds → End For Loop
10. Final Round →Mix Columns(*False*)
    a. *Sub Bytes (d_m^i)*
    b. *Shift Rows (d_m^i)*
    c. *Add Round Key(d_m^i)*
11. Data Matrix Merger →merge(d_m^i) →dE_M
12. Data Matrix Reverse validation →rvalidate(dE_M) →dE

VI. RESULTS

The image dataset is carrying total 52 images in 6 major categories. The first category of images belongs to the noisy images clicked by low resolution cameras. These images are mostly prone to the processing noises and their image quality gets more degradation that any other type of images during the matrix transform processing using the novel compression method in the proposed model. The second category belongs to the images of nature, especially beaches. These images have higher and dense color range within less basic colors.

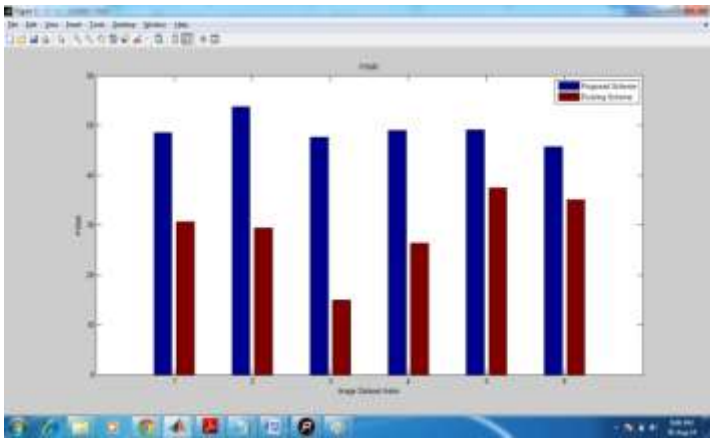

Figure 6.1: PSNR comparison between proposed and existing system

PSNR represents the quality of the image by comparing images of before and after processing on the selected image data. The above graph has clearly shown that proposed algorithm has done way better than the existing algorithm in the terms of PSNR. The PSNR value is higher in thecase of proposed algorithm than the existing algorithm for all image categories in the dataset, which shows that proposed algorithm creates clearer image at the end of the processing.

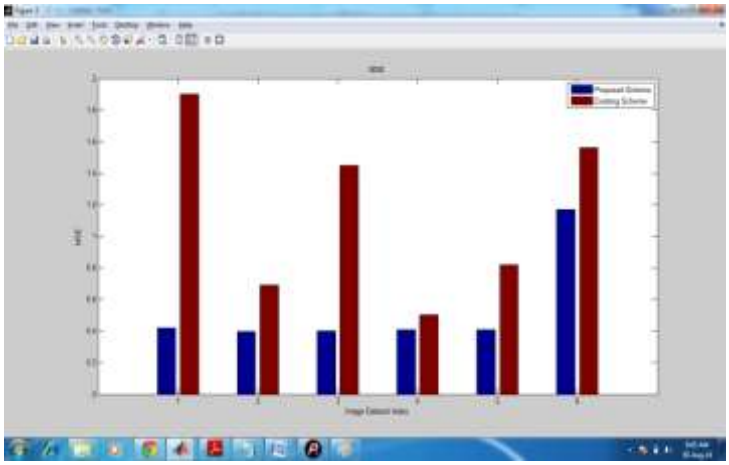

Figure 6.2: MSE comparison between proposed and existing

Mean squared error is calculated by calculating the error bits over all bits, which represents the total error in the received data when it is compared to the data sent at the other end or data before and after processing. MSE value should be less to represent the less damage to the quality of the image. In the above graph, the MSE value for proposed system is lower as compared to the existing system on different image categories in the image dataset.

VII.CONCLUSION & FUTURE WORK

The image need of picture security has been on the ascent due the ascent in the quantity of hacking endeavors each year. With the ascent of hacking endeavors over the individual information of the clients, the enthusiasm of the analysts in the security worldview has likewise emerged. The proposed display has been created as one of

the answers with the end goal of security of the picture databases. Theproposed show has been produced as the amalgamation of the three sorts of calculation: encryption, pressure and pixel concealing procedures. The proposed demonstrate has been produced with blowfish encryption instruments to ensure against the assaults. The blowfish encryption model will secure the picture information yet in addition expands the extent of the information, which requires additional storage room on the online assets. To diminish the effect of increment in estimate, the proposed demonstrate has been furnished with the pressure model to lessen the picture measure before encryption, which has been discovered powerful for the keep an eye on the information measure factor. The proposed display has been included with an additional layer of security by including the pixel concealing strategy by utilizing the obscure guide based obscuring technique. The pixel-concealing strategy has been utilized to shroud the real detail of pixels so as to shield the picture information from the hacking endeavors over the encryption display. The additional layer of pixel concealing strategy has added the additional security to the proposed show. The proposed show comes about have been assessed as picture quality parameters of pinnacle flag to clamor proportion, mean squared blunder, pressure, encryption speed and throughput. The proposed demonstrate has been discovered viable on the premise of results assessment of the proposed show against the current models.

In Future, it can be enhanced or improved by utilizing the diverse systems of security as encryption, pixel covering up or some other sort of strategies. The proposed model can be additionally improved by offering multi-layered encryption and pressure by utilizing the different encryption and pressure strategy together in the blend to frame the layered model for picture security.

REFERENCES

1. Al-Hilo, Eman A., and RusulZehwar. "Fractal Image Compression by YIQ Color Space." In *Computational Science and Computational Intelligence (CSCI), 2014 International Conference on*, vol. 1, pp. 221-225. IEEE, 2014.
2. Marcelloni, Francesco, and Massimo Vecchio. "A simple algorithm for data compression in wireless sensor networks." *Communications Letters, IEEE* 12, no. 6 (2008): 411-413.
3. JasleenKaur and DeepankarVerma,"stegnography technique"(May 2014) .
4. Dolfus, Kirsten, and Torsten Braun. "An evaluation of compression schemes for wireless networks." In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, pp. 1183-1188. IEEE, 2010.
5. Rashi Singh and GauravChawla,"A Review on Image Steganography" (May 2014)
6. Liang, Yao. "Efficient temporal compression in wireless sensor networks." In*Local Computer Networks (LCN), 2011 IEEE 36th Conference on*, pp. 466-474. IEEE, 2011.
7. MamtaJuneja and Parvinder S. Sandhu ,"An Improved LSB Based Steganography Technique for RGB Color Images"
8. Paar, Christof. "Applied cryptography and data security." *Lecture Notes), Ruhr-Universität Bochum (http://www. crypto. ruhr-uni-bochum. de)* (2000).

9. Hager, Creighton TR, Scott F. Midkiff, Jung-Min Park, and Thomas L. Martin. "Performance and energy efficiency of block ciphers in personal digital assistants." In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pp. 127-136. IEEE, 2005.
10. Kessler, Gary C. "An overview of cryptography." (2003).