ISSN 2395-1621

A Survey on Data Harboring Approach for Heterogeneous Network Security

[#1]Shubham Choudhary, [#2]Nikhil Gandhi, [#3]Aditya Anthony, [#4]Rahul Kolte,
[#5]Prof. Ganesh Bandal

[1]shubhamchoudhary13695@gmail.com
[2]nikhil.gandhi157@india.com
[3]aditya.anthony7@gmail.com
[4]kolterahul1995@gmail.com

[#1234]Department of Computer Engineering,
[#5]Prof. Department of Computer Engineering,
GHRCEM,
G.H.Raisoni College of Engineering and Management, Pune

ABSTRACT

Multimedia security is an important field of research in the area of information sharing. Now-a-days data security is very important and high priority topic. As communication is needed in computer technologies of new world. There is a huge data transaction in smartphone, internet, TV, teleconferencing, telemedicine, pervasive devices and military applications. To protect the confidentiality, integrity and authenticity of data, Encryption is one of way to give the security for data; in this regard we propose a hybrid approach for data encryption. This paper presents a survey of over various research papers dealing with data and image encryption techniques in which each technique has its own merits and demerits. It additionally focuses on the functionality of data decryption and encryption technique.

Keywords: Multimedia Security, Mapping, Scan Patterns, Encrypt data, Decrypt data.

ARTICLE INFO

Article History

Received: 21th January 2016

Received in revised form :

21th January 2016

Accepted: 24th January, 2016

Published online :

24th January, 2016

I. INTRODUCTION

Over the computer network multimedia data are shared among connected users almost every day. The most known application of multimedia technology and increasingly transmission ability of network gradually leads us to acquire information lucidly through multimedia data. The Sharing of multimedia data has been increasing rapidly these days. Today more than 62% of total commercial transactions are done online of which 27% is done on smartphone, so this field required a high quality of security. The data encryption provides a reliable and secure to transmit the data securely over the network so that no unauthorized user is able to access the data. Due to the unauthorized access attack on data available on internet (the privacy of data over the computer network is compromised, to overcome such limitation strong efficient encryption techniques are required which), has given a solid base for developing more efficient, complex and secure encryption techniques.

II. RELATED WORK

Jing-Jang Hwang et al., has proposed a business model for cloud computing for data protection using data decryption and encryption algorithms. In this method cloud service provider is responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for processing of data on cloud server. The biggest disadvantage of this method is, there is no control of data for data owner i. e, data owner has to completely trust cloud service provider and he has more computational complexity. While much effort has been required securing network communications, security of stored data remains a largely neglected area both in the development and use of such systems. Nonetheless, various implementations of encrypting file systems exist. We first concentrate on some common design models and then describe some commonly used systems. The choice of the basic design approach influences the security, performance and usability features provided by these systems.

III. EXISTING SYSTEM

A. Image Encryption Using Scan Patterns

This method converts a 2D image into a 1D list, and employs a SCAN language [7] to describe the converted result. In this language, there are several SCAN letters. Each SCAN letter represents one kind of scan order. Different kinds of combinations of SCAN letters may generate different kinds of secret images. After determining the combination of SCAN letters, the scheme then generates a SCAN string. This string defines the scan order of the original image. Next, this method scans the original image in the determined order and, moreover, encrypts the SCAN string by using commercial cryptosystems. Since the illegal users cannot obtain the correct SCAN string, the original image is therefore secure. There is no image compression in this method. Therefore, the size of the image is very large, and thus it is inefficient to encrypt or decrypt the image directly.

B. Partial Image Encryption Method

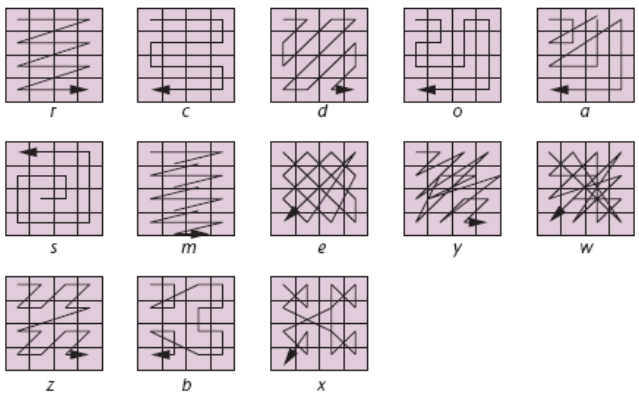
Before The following steps are involved in this method
Step 1: Select the basic mapping image or mapping image based on the SCAN pattern

Step 2: Convert every pixel of the image to be encrypted into its equivalent 8-bit binary number.

Step 3: Re-arrange the 8-bit binary number into 4-bit higher and lower nibble number.

Step 4: convert these two 4-bit nibbles into its equivalent decimal value.

Step 5: With the help of these two decimal values pickup the gray pixel from the mapping image. Where higher nibble equivalent decimal value acts as row indicator and lower nibble equivalent decimal value acts as column indicator for mapping image.
Decryption follows the reverse process of the encryption.



(a)

IV. PROPOSED SYSTEM

It is Client-Server Based Model. In which Server is responsible for servicing the requests form the client side and performing following tasks:

Authentication.
Encryption.
Decryption.

Users can access server from any device(eg: cell phone, laptop, etc.).
There are two categories of users:

Registered Users:
These users have the authority to perform encryption and decryption.

Guest Users:
These users use OTP(one time password) to decrypt the file which is shared by the registered user. These users can only decrypt file.

I. Encryption

Step 1: Create a user account. In your account Set your profile image which will serve as your client image while encryption process.

Step 2: Select and upload the file you want to encryption.

Step 3: Add a remark. After adding the remark a key will be generated and encryption process will start on server.

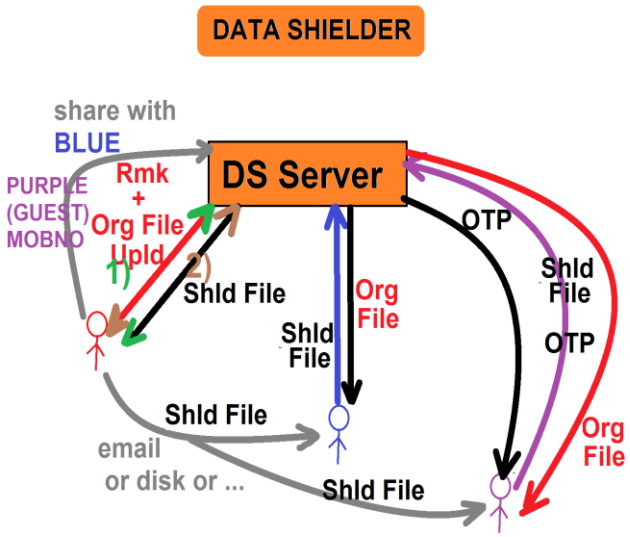
Step 4: Once your file is encrypted, download will be available.

II. Decryption

Step 1: Upload the encrypted file and select the remark necessary.

Step 2: The Decryption process will be carried out of server and it will return you the original file.

Step 3: Download and save the original file.



V. Conclusion

The security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently. To avoid reading, alteration of data, adding false information or deleting part of data, encryption is needed. So it is necessary to develop new and evolving encryption technique which are fast and secure with high rate of security.

REFERENCES

[1]Jing-Jang Hwang, Taoyuan, Taiwan,Yi-Chang Hsu, Chien-Hsing Wu, ABusiness Model for Cloud Computing Based on a Separate Encryptionand Decryption Service, in International Conference on InformationScience and Applications (ICISA), pages 1-7, 2011.

[2] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", The Journal of Systems and Software 58 , 83-91,2001.

[3] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003.

[4] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27, 2007.

[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34,1229- 1245,2001.

[6]Qais H. Alsafasfeh , Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011.

[7] Panduranga H T and Naveen kumar S K , " Hybrid Approach to Transmit a Secrete Image", 2011.

