RESEARCH ARTICLE OPEN ACCESS

A Novel Image Encryption and Decryption in Cloud

G.Bharathikannan*, M. Kalaimakal**

*(Asst Professor CSE, Sembodai Rukmani Varatharajan Engineering College, and Sembodai
Email: bharathi348@gmail.com)

** (PG Scholar CSE, Sembodai Rukmani Varatharajan Engineering College, and Sembodai
Email: kalaimakalcse2000@gmail.com)

--************************----------------------------------

Abstract:

These In today's world data security is the major problem which is to be face. In order to secure data during communication, data storage and transmission we use Advance encryption standard (AES). AES is a symmetric block cipher intended to replace DES for commercial applications .it uses 128-bit block size and a key size of 128, 192, or 256 bits. The AES algorithm is use to secure data from unauthorized user. The available AES algorithm is used for text data as well as for image data. In this paper an image is given as input AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and original image is regained as output. The AES algorithm for image encryption and decryption which synthesizes and simulated with the help of Java software for image encryption java code is synthesized and simulated by Java Application Platform SDK. Mainly Code Block Chaining (CBC) mode with PKCS 5 padding is used for image encryption.

Keywords — **Encryption, Decryption, AES,DES,CBC,SDK.**

--************************----------------------------------

I. INTRODUCTION

The uses of devices such as computer, mobile and a lot of more other device for contact as well as for data storage space and transmission has increases. As a result there is raise in no of user's also there is increase in no of unauthorized user's which are trying to right to use a data by unfair means This a rises the trouble of data security. To solve this problem a data is stored or transmitted in the encrypted arrangement. This encrypted data is incomprehensible to the unauthorized user. Cryptography is a science of information security which secures the data even as the data is being transmitted and stored. Every encryption and decryption process has two aspects: the algorithm and the key use for the encryption and decryption. yet, it is the key used for encryption and decryption that makes the procedure of cryptography secure. There are two types of cryptographic mechanisms: symmetric key cryptography in which the similar key is use for encryption and decryption. In case of asymmetric key cryptography two dissimilar keys are used for encryption and decryption. Symmetric key algorithm is a large amount faster and easier to apply and required less processing power as balance to asymmetric key algorithm. Due to increasing use of computers, now a day security of digital information is most important issue. interloper is an unnecessary person who reads and changes the information even as transmission occurs. This activity of intruder is called intrusion attack. To avoid such attack data may be encrypted to a few formats that is unreadable by an unauthorized person. AES is mainly advance edition of data encryption standard (DES).

2. LITERATURE REVIEW

C. P. Wu, C.C. J. Kuo [2], discussed with the fast growth of multimedia processing technologies and the broad availability of network right to use enable, many powerful and inspired new applications. Digital audiovisual contents can be created, edited, distributed, shared and stored with ease at a very low cost that has not at all been experienced before. On one hand, new technologies help individuals to reach better communications with one another, and facilitate artists to produce artwork of the multimedia format and distribute them to a wider vary of people via the Internet. On the other hand, because the emerging Internet is an open network which is in danger to eavesdropping, the horror that the multimedia data transmitted during the Internet could be manipulated or stolen is inhibiting the evolution of audiovisual Internet applications. Internet telephony, Internet conferencing, Internet security camera and multimedia databases are a little examples of promising audiovisual data applications that need confidentiality. The quick and efficient multimedia encryption technology is essential for Internet multimedia applications to achieve their full potential. Conventional cryptography accomplishes confidentiality by encrypting binary data with symmetric ciphers and exchanging keys with public-key encryption.

They have been mostly developed for text data and below the assumption that every bit of data in the bit stream is just as vital as others. Although encrypting the entire audiovisual data stream with cryptographic ciphers achieves utmost security, the large size of audiovisual data requires a considerable quantity of computation power. Since audiovisual data regularly have much lower information value concentration (information value per data size) than alphanumeric data, enciphering schemes with a lesser computational cost is desired. Traditionally, practical solutions to audiovisual data confidentiality are scrambling techniques, which are regularly relatively easy permutations or affine transformations in the time or the occurrence domain. As the computing power obtainable to the public increases exponentially, these scrambling algorithms turn into vulnerable to attacks. in addition, scrambling the raw signal degrades the presentation of multimedia compression systems, which are designed based on the characteristics of unscrambled signal. Therefore, we need fresh methods for audiovisual data confidentiality to achieve a high security level equal to that of cryptographic ciphers while maintaining a significantly lower computational cost at the same time. Selective encryption is based on the principle that valuable information (i.e. the content) in audiovisual data is not equally widen over every bit of the data. regularly, the content density of audiovisual data is a large amount sparser and extra unevenly distributed than text data. The goal of audiovisual data security should aim at protecting the fulfilled of the data, not the binary bit stream itself. Faster algorithms can be residential by selectively encrypting only a few part of the bit stream

2.2 Double Random Fractional Fourier-Domain Encoding For Optical Security

G. Unnikrishnan , Kehar Singh,[4],discussed with the partial Fourier transform is a generalization of the normal Fourier convert with an order parameter a. A Fourier transform is a first-order fractional Fourier transform with a51. This overview of the Fourier transform has opened up new applications and provided deeper insights in each area where the Fourier transform plays an vital role.1,2 capable algorithms have been proposed to calculate fractional Fourier transforms in about the similar time as ordinary Fourier transforms.3 visual implementations based on largeness systems have also been proposed.4 So the generalization of the normal Fourier transform to the fractional Fourier transform comes at no extra cost in digital computation or optical implementation. In the present work, we suggest a new optical encryption technique using fractional Fourier transforms. Javidi5 proposed a broadly used and highly victorious optical encryption technique referred to as twofold random Fourier-plane encoding. In this method, the data to be encrypted in the input plane is multiplied by a chance phase function. A Fourier transform is in use and multiplied by a second random part function referred to as the key statistically free of the first, in the encryption level surface.

A second Fourier transform gives the encrypted information in the output plane. freshly, an encrypted memory using a random phase mask in the Fresnel domain was also planned.6Our way may be viewed as a generalization of the dual random Fourier-plane encoding method, in the logic that the input plane, the encryption plane, and the output plane are part Fourier domains linked to each other by a fractional Fourier transform. To decrypt the data properly, one needs to detail the fractional domains in which the input plane, encryption plane, and output planes survive. Thus, one wants to give the orders of the fractional Fourier transformations relating them, in adding to the key used for encryption. In the following conversation, we offer a theoretical framework for the proposed method and recommend an optical execution. We also there some results obtained starting the computer simulation of the proposed process .We offer a new optical encryption method using the fractional Fourier transform. In this method, the data are encrypted to a stationary white noise by two statistically independent random stage masks in fractional Fourier domains. To decrypt the data suitably, one wants to specify the fractional domains in which the input plane, encryption plane, plus output planes exist, in adding together to the key used for encryption. The utilize of an anamorphic fractional Fourier convert for the encryption of two-dimensional data is also discussed. We recommend an optical implementation of the planned idea.

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

System analysis is the on the whole analysis of the system previous to implementation and for arriving at a precise solution. Careful study of a system before accomplishment prevents post implementation problems that may arise due to bad analysis of the problem statement.

Thus the requirement for systems analysis is justified. Analysis is the first essential step, detailed study of a variety of operations performed by a system and their relationships within and outside of the system. study is defining the boundaries of the scheme that will be followed by plan and implementation.

For the cryptographic procedure there exist lots of algorithms and methods. This section briefly talk about on the substitution method encryption and decryption procedure. The algorithms such as symmetric key encryption also explained in the next section:

A. Symmetric Key Encryption

The most vital kind of the encryption type is the symmetric key encryption. In the symmetric key encryption together for the encryption and decryption procedure the same key is used. Hence the privacy of the key is maintained and it is reserved private. Symmetric algorithms have the benefit of not consuming too a large amount of computing power and it workings with high speed in encryption. A block cipher is taken as the input, a key and after that the output block will be similar in size in the symmetric key encryption. The symmetric key encryption takes position in two modes either as the block ciphers or as the watercourse ciphers. In the block cipher mode the entire data is divided addicted to number of blocks and based on the block span the key is provided for encryption.

3.1.1 Disadvantages

- In Existing the time in use too much for encryption and decryption of images

- It is one of the main problem

3.2 PROPOSED SYSTEM

In proposed by using AES algorithm to encrypt and decrypt imagery in cloud simply. Many people face trouble while decrypting the encrypted data as the KEY used for encryption if stored as String in database next it becomes very hard to use that string as the KEY. So below is the code where you just need to store the encrypted code and not the key. The decryption will get place as an when wanted. For encryption we have to use a secret key all along with an algorithm. In the following case we use an algorithm called AES 128 and the bytes of the word "The Best Secret Key" as the top secret key (the best secret key we found in this world). AES algorithm can use a key of 128 bits (16 bytes * 8); so we chosen that key.

3.2.1 Advantages

- It saves time.
- effortlessly encrypt the images
- simply decrypt the images

4. ARCHITECTURE DIAGRAM

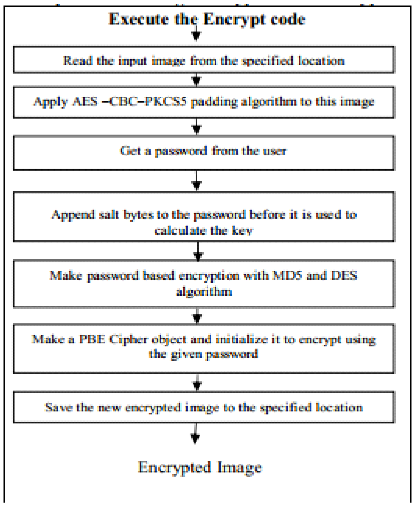
Execute the Encrypt code
Read the input image from the specified location
Apply AES –CBC–PKCS5 padding algorithm to this image
Get a password from the user
Append salt bytes to the password before it is used to calculate the key
Make password based encryption with MD5 and DES algorithm
Make a PBE Cipher object and initialize it to encrypt using the given password
Save the new encrypted image to the specified location
Encrypted Image

Fig 1: Encryption

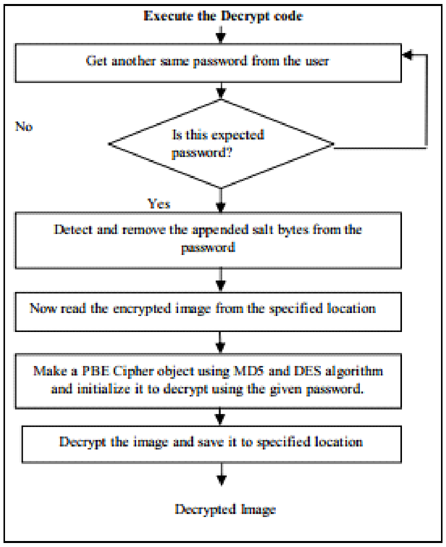
Execute the Decrypt code
Get another same password from the user
No
Is this expected password?
Yes
Detect and remove the appended salt bytes from the password
Now read the encrypted image from the specified location
Make a PBE Cipher object using MD5 and DES algorithm and initialize it to decrypt using the given password.
Decrypt the image and save it to specified location
Decrypted Image

Fig 2: Decryption

Fog computing has a distributed architecture that targets services and applications with broadly isolated deployments. Different fog computing architectures have been planned in the literature. It described a three-tier architecture where tier 1 is the bottom tier comprising of several terminal nodes (TN) (e.g., smart device and wireless sensor nodes) that send out information to the upper tiers. Tier two is the middle tier (also referred to as the fog computing layer) comprising of extremely intelligent devices, such as routers, switches and gateways.

5. SYSTEM IMPLEMENTATION

Implementation is the phase in the project where the theoretical design is twisted into a working system. The implementation stage constructs, installs and operates the fresh system. The most essential stage in achieving a new victorious system is that it will work efficiently and effectively.

There are a number of activities involved at the same time as implementing a new project.

- End user preparation
- End user teaching
- Training on the request software

5.1 SYSTEM MODULE

- Organizational Module
- Encryption Module
- Decryption Module
- File shift Module

6. Conclusion

AES encryption algorithm in CFB mode is used at this time for image encryption. PKCS5 stuffing method is used here. The relative performance advantage of code is clearly shown here. It can obviously conclude from the table 5, 6 and 7 that AES is best algorithm amongst all others. Java Application Platform SDK be release source software thus picture encryption can be offer missing investing some cost. The proposed methodology is practical for ensuring the private privacy in the context of surveillance video camera systems. Only official users that possess the key can decrypt the entire encrypted image series. The proposed method has the advantage of being appropriate for mobile devices, which at present use the JPEG image compression algorithm, due to its lesser computational necessities. The experiments have exposed that we can achieve the desired level of encryption in chosen areas of the image, while maintain the full JPEG image compression agreement, under a least set of computational requirements.

References

[1] Furht, Borko, Edin Muharemagic, and Daniel Socek "Image encryption algorithms." Multimedia Encryption and Watermarking (2005): 79-120.

[2] C. P. Wu, C.C. J. Kuo, "Fast Encryption Methods for Audiovisual Data Confidentiality", SPIE International Symposia on Information Technologies ,Proceedings of SPIE, vol. 4209,pp. 284-295, Boston, MA, USA, 2000.

[3] I. Djurovic, S. Stankovic, I. Pitas, "Digital Watermarking in the fractional Fourier transformation domain", Journal of Network and Computer Applications, vol. 24,pp. 167-173, 2001.

[4] G. Unnikrishnan, Kehar Singh, "Double random fractional Fourier-domain encoding for optical security", Optical Engineering, vol. 39, pp. 2853-2859, November 2000.

[5] C. P. Wu,C.-C. J. Kuo, "Efficient multimedia encryption via entropy codec design ",In Proceedings of SPIE, Security and Water marking of Multimedia Contents III, volume 4314, SanJose, CA, USA, January 2001.

[6] W. Zeng, S, Lei "Efficient frequency domain selective scrambling of digital video" IEEE Transactions on Multimedia vol. 5 pp.118-129, March 2003

[7] Ismet Ozturk and Ibrahim Sogukpinaar, “Analysis and Comparison of Image Encryption Algorithms” Transaction on engineering Computer and Technology 2004, vol.3, pp.38-42

[8] Komal D Patel, Sonal Belani, “Image encryption using different techniques: A review”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011.

[9] Press, W. H., Flannery, B. P., Teukolsky, S. A., Vetterling,W.T., Numerical Recipes in C: The Art of Scientific Computing, Cambridge University Press, Second Edition, Oct. 30, 1992, pp.504-510.

[10] See also M. T. Heideman, D. H. Johnson, and C. S. Burrus,"Gauss and the history of the fast Fourier transform, "IEEEASSP Magazine 1 (4), 14-21 (1984).