ISSN:0975-9646

Image Privacy Protection for Online Storage Using Adaptive Security Model

Rupinder Kaur
PURCITM,Mohali

Rekha Bhatia
PURCITM,Mohali

Abstract -- Now-a-days users access these applications from their portable devices (smart phone, tablet, etc.). To prevent the data theft from those web or mobile application architectures, there are various data security mechanism for image, video or text data. These existing security mechanisms are either using encryption or steganography, or their combinations. This paper provides of hybrid image model for cloud storage.There is various securable and perfect system of image encryption that can be well protected from unauthorized access. When it comes to the image transfers over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. To achieve the goal of image security, a number of image security and image processing algorithms are in use individually or in a combination to provide the effective image security. But these existing image security mechanisms fail to provide the best image security and sometimes proved to be breakable or hack-able. Image compression is an additional function, which can be applied on the image to lower their memory size.

Keywords: Image security, steganography, encryption, compression, DWT.

INTRODUCTION

When it comes to the image transfers over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. To achieve the goal of image security, a number of image security and image processing algorithms are in use individually or in a combination to provide the effective image security. But these existing image security mechanisms fail to provide the best image security and sometimes proved to be breakable to hack-able.

The algorithms usually used for the Image security purpose are encryption and steganography. Cryptography is the science of information and communication security. Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. It uses an cryptographic system to transform a plaintext into a cipher text, using most of the time a key. There exists certain cipher that doesn't need a key at all. An example is a simple Caesar-cipher that obscures text by replacing each letter with the letter thirteen places down in the alphabet. Since our alphabet has 26 characters, it is enough to encrypt the cipher text again to retrieve the original message.

For the encryption of images, we use a variety of symmetric or asymmetric algorithms like Blowfish, AES, DES, etc.[8] Symmetric key encryption uses same key to encrypt an decrypt, whereas asymmetric key algorithms uses different keys for encryption and decryption. For best encryption, blowfish or AES are considered the best encryption algorithm but they can be differentiated on the basis of execution speed and strong encryption standard. The blowfish is fast, but AES is more reliable and provides higher security at the core.[8]

The Advanced Encryption Standard, in the following referenced as AES, is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard was found too weak because of its small key size and the technological advancements in processor power. Fifteen candidates were accepted in 1998 and based on public comments the pool was reduced to five finalists in 1999. In October 2000, one of these five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndael.

The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a Block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key. It is important to know that the secret key can be of any size (depending on the cipher used) and that AES uses three different key sizes: 128, 192 and 256 bits.

While AES supports only block sizes of 128 bits and key sizes of 128, 192 and 256 bits, the original Rijndael supports key and block sizes in any multiple of 32, with a minimum of 128 and a maximum of 256 bits. In a world where many transactions are done over networks, attacks on the security of the data over the network have become a major concern. Cryptography is used as a tool to counter these attacks. With ever expanding technology and the increase in speeds of microprocessor chips, DES (the Data Encryption Standard) had, by the late 1990s become obsolete.

In 1997, the United States National Institute of Standards and Technology (NIST) initiated a new Encryption standard, called the Advanced Encryption Standard, which was to replace DES as the Federal Information Processing Standard (FIPS). In October 2002, after an extensive search process, a block cipher algorithm Rijndael was accepted as the new Advanced Encryption Standard. The algorithm was designed by Vincent Rijmen and Joan Daemen.

Image transfers over internet or intranet are prone to hacking. The image transferred over internet or intranet can be hacked by hackers using masquerading, man-in-the-middle or other passive attacks. Either active attacks can be used for hacking image data, in case shared or transferred data is copied or saved on server of the service provider. Active attack is term used for the attack generated by

hacker or a group of hackers to take the unauthorized access ofanyserver running the application or data storage or something else of hacker's interest.

To prevent the hacking attacks on the image storage or during transfers, image security mechanism has to be used to prevent those hacking attacks. The image security mechanisms which can be used for the image security purpose are encryption, steganography or a combination of both. End to end authentication can be also used to keep image transfer integrity intact, but end to end authentication is not possible in case of many image transfers. To provide end to end authentication security a third party application or protocol has to be installed on both sides, especially in the case of internet applications. Sometimes, the authentication requires an additional security layer in order to increase the data integrity and confidentiality on the server side storage or during internet or intranet transfers.

LITERATURE REVIEW

N. Siva Selvan have proposed a technique for Visual Cryptography with an Etched Photoengraving Practice for the purpose of image security. In this paper, a method has been proposed in which the engraved shares are error diffused continuously so that the shares can be so appealing. Error Diffusion is less complex and error filters are put to use to obtain high quality shares. This process is done through array of processors after optimal scheduling of pixels to obtain shares at a faster rate. To end with, the secret image can be retrieved by super positioning the eligible half toned shares. The image so obtained is comparatively better and is not susceptible to cross interference due to high PSNR. Zhiqianga, Li et. al. have proposed an algorithm for jpeg analysis and application in Image Compression Encryption. The authors have selected the original image to complete the Matlab simulation analysis based on JEPG algorithm. Thirdly, by using the DSP host processor, we can complete the hardware implementation of image acquisition and compression easily. Last but not least, this article selects a better compressed image to finish image encryption process. Experimental results show that JPEG image compression encryption algorithm is effectively guaranteed for the actual engineering applications and will be widely used in secure communication.

Navita Agarwal et. al. have proposed an efficient pixel-shuffling based approach to simultaneously perform image compression, encryption and steganography. In this research, authors have conducted a similar research, where they have applied compression, encryption and steganography on the digital image data. Pixel shuffling based symmetric encryption algorithm, DCT for compression, Winrar to Image steganography are used to achieve the proposed model in this paper. Riaz, Sidra, and Sang-Woong Lee have developed an Image authentication and restoration method by using multiple watermarking techniques with advance encryption standard in digital photography. In this paper, a multimedia authentication and restoration scheme is proposed with the security of AES-128 ciphered watermarking and correlated watermarking. An encrypted or ciphered image embedding is done by modified version of Closest Point Transform (CPT) in a digital photograph. We performed several security attacks e.g. noise attack, compression attack, and cropping attack on multiple watermarked photographs and evaluated the proposed watermarking technique to examine the system robustness. Image Authentication is done by locating the tempered areas and restoration is performed by correlated watermark on the tempered region of watermarked photograph. Quist-Aphetsi have worked upon cryptographic image encryption technique for facial-blurring of images. This paper proposes an image encryption technique that will make it possible for selected facial area to be encrypted based on RGB pixel shuffling of an m*n size image. This will make it difficult for off-the-shelf software to restore the encrypted image and also make it easy for the law enforce-ment agencies to reconstruct the face back in case the picture or video is related to an abuse case. The implementation of the encryption method will be done using MATLAB. At the end, there will be no change in the total size of the image during encryption and decryption process. Christopher Thorpe have developed a co-prime blur scheme for data security in video surveillance. This paper presents a novel coprime blurred pair (CBP) model to improve data security in camera surveillance. While most previous approaches have focused on completely encrypting the video stream, we introduce a spatial encryption scheme by strategically blurring the image/video contents. Specifically, we form a public stream and a private stream by blurring the original video data using two different kernels. Each blurred stream will provide the user who has lower clearance less access to personally identifiable details while still allowing behavior to be monitored.

PROBLEM INTRODUCTION

In traditional web or mobile application architectures, the cloud servers or environments acts as a database server or simple data routing server that offers connectivity between clients. Majority of these types of businesses lacks in the adequate security levels to protect the user data. On most of the social applications are mostly used to share personal data (mostly images) by its users. Hacks into these applications can cause great losses to the user security which can lower the number active user and so the business popularity.

The social application built for smart phones or desktop, which are primarily used for the personal data sharing by its users. The personal data consist of the image and text data. Most of these images are the personal images of the users, theft of which may cause a great defamation to the person's image. So these images must be made as much secure as possible. The bandwidth of the internet links used on smart phones in India are comparatively lower. Hence if data would be in the compressed form, the data transportation can be effectively utilized. Here we are proposing the combination of double layer image encryption and image blurring algorithm, which will ensure the security. The secure image storage on cloud environments is the primary requirement of such applications, where images are being transferred or

transmitted between the servers and their users. The image security is quite important because they belongs the users. The users capture their personal movements or activities in the form of images as their past memories. These images, if hacked, can be used to defame a person's social image. Sometimes, the communication between servers and users takes too much time in data transfers because of their geographical distance. The bandwidth of communications links is lower in many areas under mobile network coverage. Hence if data would be secured, the communication channel will be effectively secured.

Since the actual processing of the data takes place on the remote client the data has to be transported over the network to make it reach to the other user, which requires a secured format of the transfer method. Present day transactions are considered to be slower and "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. Secure transfer mode in the existing system is the motivation factor for a new system with higher-level security standards for the information exchange.

HYBRID IMAGE SECURITY MODEL

In this research, we have proposed a hybrid image security model for the cloud storage and communications, which will be implemented by combining various techniques together to achieve the image security goal. The techniques included in the combination would be blurring, cryptography and image compression. The proposed model has been divided into two image security components: image blurring and double layer encryption. The image blurring will lower the details of the image, which means, if a hacker will attack and download the images, he will have to work hard a lot to remove the blurring effect caused by the mathematical computations to create blur image. Then the image encryption will be used to create a completely unreadable and hashed image. A fast and robust variant of image encryption will be used for the encryption module. The double layer encryption using AES algorithm would be used for the encryption purposed for the image security for image storage and during transmission.At first stage, a detailed literature study would be conducted on the methods or architectures about the image security methods. In addition, the basic problems and requirement analysis of scene classification models would be thoroughly studied and developed. Literature study will lead us towards refining the structure of the proposed security solution design. Afterwards, the proposed solution will be implemented in MATLAB simulator and a thorough performance analysis would be performed. Obtained results would be analyzed and compared with the existing techniques.

CONCLUSION

End to end authentication can be also used to keep image transfer integrity intact, but end to end authentication is not possible in case of many image transfers, because many server based internet services like Facebook, Whatsapp, etc. does not let a user to save the content in secure formats, and does not allow the end-to-end authentication based protocols. In order to guard the image transmission, the algorithms usually used for the Image security purpose are: Compression, Encryption and Steganography. The DWT technique used for compression is more complex. However DCT is simple to implement so data can be easily access by unauthorized user [1].DCT is simple as the number of computations is less in it, because it computes cosines function at the different frequencies. DWT is complex than DCT because numbers of computations are more and it works with both, the frequency and time. For the numerical and functional analysis, DWT uses a number of options between the wavelets.

FUTURE WORK

In the future, the proposed work can be enhanced for harden and quick image security execution with the quality improvement in terms of PSNR, MSE, RMSE, etc. Also a detailed performance evaluation survey can be performed on the proposed algorithm to evaluate the real-time performance in the different scenarios.

REFERENCES

[1] Mohammadi S., Abbasimehr H., "A high level security mechanism for internet polls", ICSPS, vol. 3, pp. 101-105, IEEE, 2010.

[2] N. Siva Selvan, "Reconciling Visual Cryptography with an Etched Photoengraving Practice for an Exceedingly Secured Secret Image Sharing", ICRCC, vol. 1, pp. 260-263, IEEE, 2012.

[3] Zhiqianga, Li, Sun Xiaoxin, Du Changbin, and Ding Qun. "JPEG Algorithm Analysis and Application in Image Compression Encryption of Digital Chaos." In Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2013 Third International Conference on, pp. 185-189. IEEE, 2013.

[4] Navita Agarwal, Himanshu Sharma "An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography", IJCSMC, May 2013.

[5] Riaz, Sidra, and Sang-Woong Lee. "Image authentication and restoration by multiple watermarking techniques with advance encryption standard in digital photography." In Advanced Communication Technology (ICACT), 2013 15th International Conference on, pp. 24-28. IEEE, 2013.

[6] Kester, Quist-Aphetsi. "A cryptographic image encryption technique for facial-blurring of images." arXiv preprint arXiv:1307.6409 2013.

[7] Thorpe, Christopher, Feng Li, Zijia Li, Zhan Yu, David Saunders, and Jingyi Yu. "A Co-Prime Blur Scheme for Data Security in Video Surveillance." 2013.

[8] Kester, Quist-Aphetsi, Laurent Nana, and Anca Christine Pascu. "A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud Using AES and RGB Pixel Displacement." In Modelling Symposium (EMS), 2013 European, pp. 293-298. IEEE, 2013.

[9] Gary C.Kessler, " An Overview of Cryptography: Cryptographic", 2014.

[10] MilindMathur, Ayush Kesarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", NCNHIT vol. 1 143-148,2013.

[11] Ashwin S., "Novel and secure encoding and hiding techniques using image steganography: A survey", ICETEEEM, vol. 1, pp. 171-177, IEEE, 2012.

[12] Chanu Y. J, "A short survey on image steganography and steganalysis techniques", NCETAS, vol. 1, pp. 52-55, IEEE, 2012.

[13] Chamkour Singh, Gauravdeep, "Cluster based Image Steganography using Pattern Matching", IJAIR, vol. 2, issue 5, 2013.

[14] Verma O.P., Agarwal R., Dafouti D., "Performance analysis of data encryption algorithms", ICECT, vol. 5, pp. 399-403, IEEE, 2011.