Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Image Privacy Protection for Online Storage Using Adaptive Security Model

**Rupinder Kaur, Rekha Bhatia**
Dept of Computer Science, Purcitm,
Mohali, Punjab, India

***Abstract — The image security has been very important concern in the modern area of internet. The security breach may hurt the privacy of the users, which can be also used for the social de-facing of specific person, whom image data has been hacked. The image security also becomes very important in the case of digital media creation companies, who always stay concerned with the copyright protection. The proposed model has been designed in the double layered mechanism for the image security. The proposed model has been designed to protect the both personal data of users and digital media company image data. The proposed model has been designed to protect the user privacy as well as the copyright protection for the user data and digital data, respectively. Our approach offers the double layered encryption mechanisms over the image using the blowfish algorithm. The blowfish algorithm has been found very efficient and quick during our literature survey on the image encryption model, but it carries a little security loophole against the cryptanalysis attacks, which has been mitigated through the double layered mechanism proposed in this paper for the purpose of the image security. The proposed model has been combined with the visual distortion controller method, which directly applies the blur over the image to hide the visual details of the image. The proposed model has been found efficient in comparison with the existing models in the terms of speed and throughput.***

***Keywords: Double layered blowfish encryption, chaotic-map based pixel abstraction, image security, encryption, blowfish.***

## I. INTRODUCTION

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in
the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature.

Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure- correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

 

Digital multimedia is data can be delivered over the computer networks, which is prone to the security breaches. The countries launch the space missions to get the information about the existing elements in the space. The countries don't want the information to get leaked. So there must be security mechanism which can ensure the security of inter-space transmissions. Under this research we are proposing secure mechanism to secure the images in the inter-space communications. As we know that, digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of the countries and space agencies own that data. Hybrid image security is a solution to the problem. It includes a combination of steganography, cryptography and compression.

The proposed model has been designed to use the blurring or visual details abstraction method alongside the encryption mechanisms using the blowfish algorithm. The proposed model has been designed for the security of the personal data of users and well as the image copyright protection for the digital media houses.

## II. ALGORITHMS USED

**1.1. Encryption Algorithm:** The advance encryption standard has been used for the purpose of encryption in the proposed model. The AES algorithm is a symmetric encryption model based encryption used to encrypt the various forms of data in the different round formation. The proposed model is using the 128-bit key length based encryption algorithm with the 128-bit block size and with 10-encryption rounds. The AES cipher has been defined step by step in the following figure:

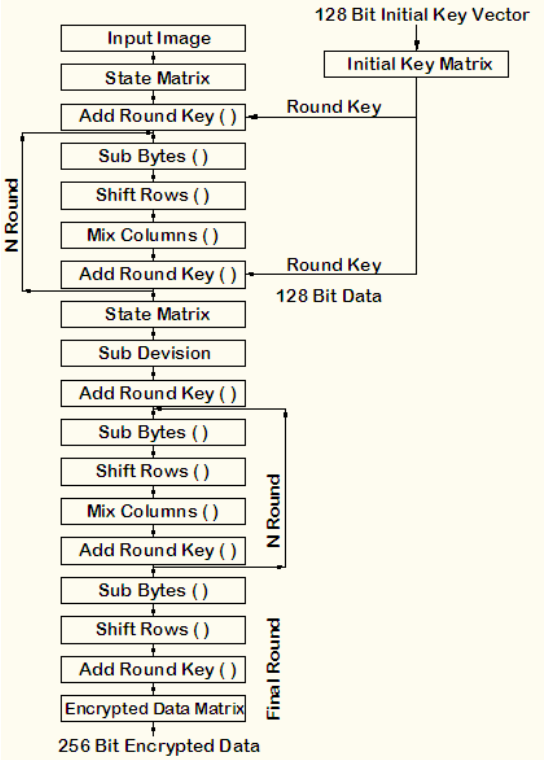


Figure 2.1: The AES cryptographic algorithm design

**1.2. Blurring Algorithm for Pixel Details Abstraction:** The proposed scheme is a modification of the one suggested by Lian et al.[8]. In their blurring algorithm, an explicit diffusion function based on a logistic map is used to spread out the influence of a single plain image pixel over many cipher image elements. Although the diffusion function is executed at a fairly high rate, it is still the highest cost, in terms computational time, of the whole blurring algorithm. This is because multiplications of real numbers are required in this stage. Table 1 lists the time required in different parts of Lian et al's blurring algorithm. It shows that the time for completing a single diffusion round is more than four times longer than that for a permutation. The shift operation can also be performed before addition. However, simulation results found that the "add and then shift" combination leads to the best performance and so it becomes the choice in our blurring algorithm. The new pixel value is then given by Eq. (5). [ ] ( )mod , ( ) i = i + i−1 3 i−1 v Cyc p v L LSB v (5) where pi is the current pixel value of the plain image, L is the total number of gray levels of the image, vi-1 is the value of the (i-1)th pixel after permutation, Cyc[s, q] is the q-bit right cyclic shift on the binary sequence s, LSB3(s) refers to the value of the least three significant bits of s, vi is the resultant pixel value in the permuted image. The seed [ ] 0, 1 v−1 ∈ L − is a sub-key obtained from the key generator.

As the pixel value mixing depends on the value of the previously processed pixel, the operation sequence cannot be changed. This may lead to a problem in the reversed confusion process required in deblurring. A solution is to make the first decipher round perform the reverse position permutation only. Then both reverse position permutation and pixel value change are performed from the second decipher round. In this manner, an additional deblur round is required for the reverse of pixel value modification. It composes of the simple add-and-shift operation and adds only little cost to the overall deblur procedures.

 

## III. RELATED WORK

**Eman A. Al-Hilo, Rusul Zehwar [2014] have proposed** the fractal compression technique proposed by Jacquin is investigated for 24 bits/pixel color image. The data of the color component (R,G,B) are transformed to (YIQ) color space, to take the advantage of the existing spectral correlation to gain more compression. Also the low spatial resolution of the human vision systems to the chromatic components (I,Q) was utilized to increase the compression ratio without making significant subjective distortion. The test results show that PSNR (31.05) dB with CR (8.73) and encoding time (57.55) sec for Lena image (256x256) pixel.

**Henry Ponti Medeiros et al. [2014]** have been focused on lightweight compression mechanism for low resolution sensor nodes based on fixed Huffman dictionaries. Since the proposed scheme presents very modest computational and memory requirements, it can be easily employed in practical wireless sensor nodes. In order to evaluate the method, they have computed the compression ratio obtained in several real datasets containing temperature and relative humidity measurements collected at different locations and during distinct periods of time. The compression ratios obtained using this approach varies between 46% and 82%.

**Xiangui Kang, Jiwu Huang [2003]** have proposed the water marking extraction has been demonstrated for JPEG compression. In watermark extraction, authors at first detect the template in a possibly corrupted watermarked image to obtain the parameters of affine transform and convert the image back to its original shape. Then they have performed translation registration by using the training sequence embedded in the DWT domain and finally extract the informative watermark. Experimental works have demonstrated that the watermark generated by the proposed algorithm is more robust than other watermarking algorithms reported in the literature. Specifically it is robust against almost all affine transform related testing functions in StirMark 3.1 and JPEG compression with quality factor as low as 10 simultaneously. While the approach is presented for gray-level images, it can also be applied to color images and video sequences.

**Sonja Grgic, Mislav Grgic [2001]** have examined a set of wavelet functions (wavelets) for implementation in a still image compression system and to highlight the benefit of this transform relating to today's methods. The paper discusses important features of wavelet transform in compression of still images, including the extent to which the quality of image is degraded by the process of wavelet compression and decompression. Image quality is measured objectively, using peak signal-to-noise ratio or picture quality scale, and subjectively, using perceived image quality. The effects of different wavelet functions, image contents and compression ratios are assessed. A comparison with a discrete-cosine-transform-based compression system is given.

## IV. PROBLEM FORMULATION

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.

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.

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.

## V. PROPOSED RESEARCH 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 three major components: Encryption, Blurring and Compression. The compression scheme will reduce the size of the images to be stored. 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 table is representing the results of the proposed algorithm on the selected image dataset. 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 blurring 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. For example, the image carrying the scene of ocean is having multiple color densities of blue color in them, which are more prone to loss of the details during the processing. The third types of the images are green infrastructure, which are carrying less number of colors than the other images. These images are less prone to the system of transmission noises. The fourth type of images belongs to the urban transportation category. These images are representing on dominant color over the other, hence the effects of processing and transmission noises effects on one color can be studied. The fifth type of images belongs to the digital image category. The digital images fall in the noisy image category. The human cannot determine the noise in these images. But, sometimes, the noise degrades the image quality at a large. The sixth type of images is grayscale image

## VI. RESULT ANALYSIS

Table 1: The comparison of images of various categories in the Image dataset

| **Image Group in Dataset** | **Images** | **PSNR** | **ET** | **MSE** |
|---|---|---|---|---|
|  | 0-7 | 48.58 | Com: 0.420 | 1.23 |
|  | 8-19 | 53.76 | Com:0.398 | 0.54 |
|  | 20-29 | 47.61 | Com: 0.40 | 1.82 |
|  | 30-39 | 49.01 | Comp: 0.41 | 0.88 |
|  | 40-49 | 49.14 | Comp: 0.408 | 1.98 |
|  | 50-52 | 45.68 | Comp: 1.168 | 2.10 |

The sizes shown in the table 2 are the real sizes of the images stored on the disk. The performance of the proposed algorithm can have slight variations on each performance test because of the variation in the CPU usage and RAM usage on the PC due to operating system or other processes.

Table 2: Mean of the results of improved AES implementation on dataset of 50 images

| | |
|---|---|
| Average File Size | 948 Kb |
| Average Encryption Time | 2 seconds |
| Average Decryption Time | 0.64 seconds |
| Average Encryption Speed | 472 Kb/second |
| Average Decryption Speed | 1474 Kb/second |

The proposed algorithm has been proved to be way faster than the existing AES algorithm. The existing algorithm is taking almost 3-5 times slower than the proposed algorithm. The proposed algorithm has been proved to be efficient for both image and text data.

 

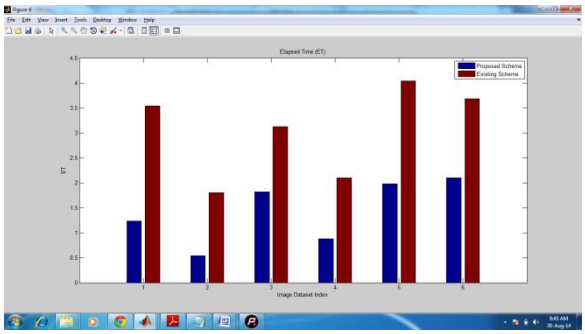


Figure 1: Elapsed time between proposed and existing system

Elapsed time is the total time taken by system to execute its operations for blurring mechanism on the selected data. The above graph has clearly shown that proposed algorithm has done way better than the existing algorithm. The elapsed time of the proposed algorithm is lower for all image categories in the dataset.

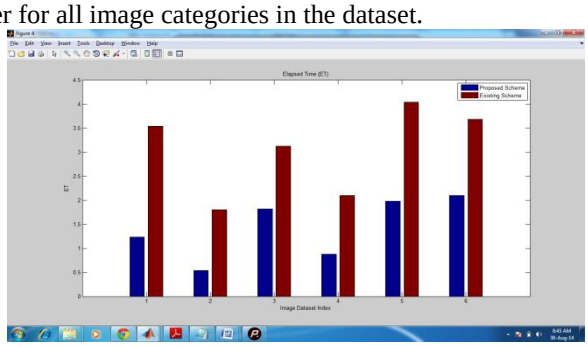


Figure 2: PSNR comparison between proposed and existing system

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 the case 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.

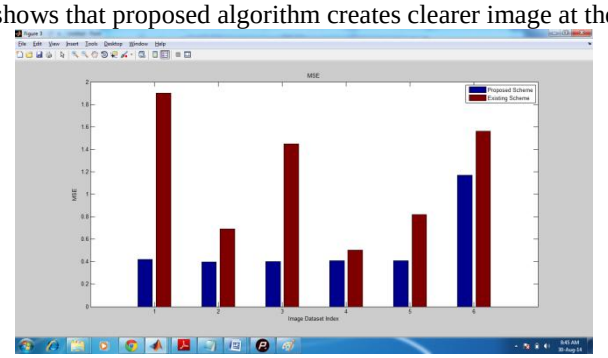


Figure 3: MSE comparison between proposed and existing

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.

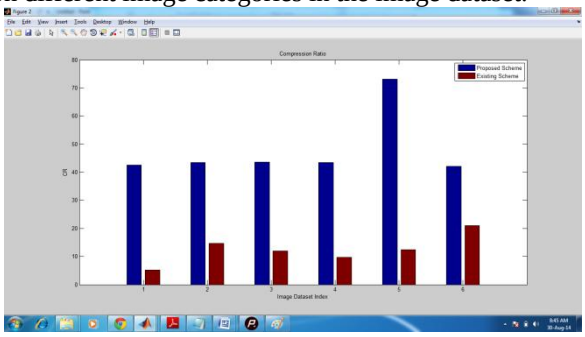


Figure 4: Blurring Ratio based comparison between existing and proposed system

Blurring Ratio represents the reduction in the size of the image after the blurring process. Higher is the blurring ratio; lower is the transmission effort and disk space consumption. In the case of proposed model, the blurring is recorded way higher than the existing model.

 

## VII. CONCLUSION

In this paper, we have defined the new image security mechanisms using the chaotic-map based pixel abstraction along with double-layered blowfish encryption to add the robustness to the image security. The proposed model is efficient for the digital media houses and the online users to protect their image data stored on the online resources. The proposed model has been designed to mitigate the threats caused by the possible attacks over the online image data stores. The proposed model has been evaluated on the basis of PSNR, MSE, Encryption speed, etc. The proposed model has been found efficient and effective in comparison with the existing models.

## ACKNOWLEDGEMENTS

I take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this project.

I would like to show my greatest appreciation to Mrs. Rekha Bhatia. I cannot thank her enough for her tremendous support and help. I felt motivated and encouraged every time I discussed the work with her. Without her encouragement and guidance this project would not have materialized. She played a key role in guiding me through this endeavor. She has always been very flexible. It has been my proud privilege to have an opportunity to work and learn under her inspiring and stimulating guidance.

My heartfelt gratitude and indebtedness goes to all my friends for guidance with their encouraging, caring words, constructive criticism and segmentation have contributed directly or indirectly in a significant way towards completion of this training. My special thanks to go my friends whose support and encouragement have been a constant source of assurance, guidance, strength and inspection to me.

I am immensely grateful to my parents, my family. They have always supported me and taught me the things that matter most in life. I am proudly grateful to all of them.

## REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

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

[6] 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): 1-1.

[7] 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.

[8] Gary C.Kessler, " An Overview of Cryptography: Cryptographic", 2014. http://www.garykessler.net/library/crypto.html#intro

[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.

 