International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 13803-13811

http://www.ripublication.com

A New Approach To Chaos Based Image Encryption Using Confusion and Key As Image

Dipti Chandrakar
School of Information Technology
Vellore Institute of Technology
Vellore, Tamil Nadu
dipti.chandrakar@gmail.com
Asha B Patil
School of Information Technology
Vellore Institute of Technology
Vellore, Tamil Nadu
ashabpatilp@gmail.com

Abstract

In recent year, every information is store in the untrusted cloud. In cloud major threat is security management system. Cloud has many sensitive data such as images, videos etc. In this paper, a new image encryption technique is proposed based on chaos-based key generation followed by confusion technique and then bitXOR with scramble key image. It is implemented on Matlab 2010. For results we use histogram and entropy information which tells that there is no information loss as well as resist attack on image.

Keywords: Image encryption, chaos, key image, confusion technique

Introduction

With the increasing demands for the fast growing information technologies and Communication channel across the internet more and more digital audios, images and videos are transmitted through the wireless networks .Many information related to image is being share through many social networks like facebook, flickers and e-mails. It has been estimated that cloud computing in various fields like health care ,social networking ,defense sector, e-mail etc will reaches $6.9 billion by 2017[1].In future many company are moving to cloud for data storage and processing. The switching to the cloud add many advantages for cloud users like scalability, availability ,high performances ,elasticity and speed, no data loss ,cost effective etc all this features make cloud so popular and in future it will grow tremendously because of the above benefits. Apart from it's advantages cloud has many disadvantages also

like storing and processing many sensitive medical or defense data etc over the cloud .In addition to storing and processing, the data security and confidentiality are the main challenges. Data breaches charged the health care industries or defense sensitive data about $8 billion annually. Preserving the confidentiality about the sensitive data is the important factor in cloud computing. One way of preserving the confidentiality of the sensitive data is by encode the image data before uploading it into the clouds. The encryption techniques is feasible but it has two drawback(i)high processing is required for both encrypting and decrypting the image data and (ii) computing on encrypted data is highly inefficiencies.

Big image encryption and decryption at every retrieve from the cloud can be restricted for resources confined mobile devices. One way of minimizing this problem is by offloading the encryption and decryption operations themselves in the cloud. Sometimes this offloading operation is not a feasible solution for sensitive information such as medical images. In addition to offloading operation problem another problem is difficulty in computation on encrypted data. Approaches used in homomorphic encryption schemes (FHE) [2] is very difficult to adopt for practical use because of high cost computation of FHE.

Chaos has unique characteristic like system dependency, ergodicity, quasi-randomness on parameters of system and initial conditions, have granted an novel approach for image encryption algorithm .The chaos based encryption algorithm is fast .In recent years , many chaos –based encryption scheme have been proposed ,but still high security is not achieved. The features of the chaos-based scheme have draw the attention of many cryptographer to proposed new encryption algorithm with higher speed and security.

This paper introduces a new approach for preserving the security of the image before uploading into the clouds. The proposed image encryption scheme use chaos based approach. Recently so many image encryption technique has proposed [3],[4],[5], to confuse image data we use chaos based key generation, confusion technique and key image. We eliminate diffusion because we needs efficient retrieval to original pixel of data and makes the encoding scheme simple.

Related Work

The scheme proposed by [6] where compression of JPEG is based on tolerant DCT image encryption scheme, where proposed scheme has two features. First if encrypted image is compressed using JPEG than decryption algorithm is used to recreate image of plaintext. Secondly by adjusting the encryption algorithm it is possible to produce variable perceptual distortion of cipher-image. This proposed method uses orthogonal matrices.

The scheme proposed by [7], where image encryption and decryption takes based on the RGB pixel used in cryptographic application by using cryptographic technique. In this method where bit values have no changes. Here numerical values of respective position are shifted away and the values of RGB are interchanged.

The scheme proposed by [8], where encoding of image process starts with input image and secret keys specified by user. The scheme creates mask image by

extracting random filer images where flicker image has their own id in cloud database. To obtain encoded image it being done by chaotic map transformation.

The scheme proposed by [9] where enhance the protection by encryption which is based on operation of permutation and diffusion is performed. Original image is divided into pieces blocks and permuted. To obtain scrambled, the principle is applied on each block. In scrambled image is pixel values can be changes, than apply XOR operation on row and column separately in order to achieve high security.

The scheme proposed by [10] where plain image has message authentication code which is of 512 bit is transformed to 64 bytes, it is then replaced by pixels of image. Technique called Reversible data embedded is used on replaced pixel to embed into image and then using pseudo sequence feedback mask the embedded image. To generate message authentication code, Key hashed function is used. After Decryption the information is extracted which was embedded. As image first 32 pixels is being replaced this is vulnerable to attack.

The scheme proposed by [11] where the approach uses substitution and diffusion. There are 16 rounds. First, image is divided into blocks where session key is used for deciding the size of block during encryption process at each round. On each block Diffusion is performed on image by rearranging the image pixel in zig-zag path. Substitution process where in pixels of each block is altered based on properties of another pixels this is performed by XOR with adjacent pixel this produces current pixel. Mixing process, here mixing pixel of present image pixel with previous pixel to get new pixel along with session key.

Proposed Work

The fig 1 better explains our proposed work. In our scheme we first compare size of the original image and key image. After applying confusion technique we will get blurred image. The encrypted image is obtained by bitXOR blurred image with scrambled key image. For obtaining decrypted image reverse operation is performed.

A. Methodology

Comparison of images

Here original image size is compare with key image size. If it matches then it will perform the below operation other wise it will search for another key image .

Chaos-based Key Generation

Initialize the value for x0, y0,k and n value. Then calculate the value for Key(1),Key(2),Key(3),Key(4). For generating Key(1) find the floor value of (x0/360) then multiply with 256. For generating Key(2) find the floor value of (y0/360) then multiply with 256. For generating Key(3) find the floor value of mod(k,256) . For generating Key(4) find mod of (n,256) .

Confusion Technique

Confusion is obtained by bitXORing 1st pixel data of red channel of the original image with key (1), 1st pixel data of green channel of the original image with key (2), 1st pixel data of blue channel of the image with key (3). 2nd pixel data of red channel of original image with key(4), then 2nd pixel of green with key(1) and so on it iterates. After confusion by chaos based key we will get confused image, the confused image is then divided into two part after each iteration. If(part1>0) and (part2>0) then the confused image is assign to new array else bitXOR original image with the confused image and then assign to new array. If above condition fails then again check condition for part2<0 then the confuse image is assign to new array else bitXOR original image with confused image and assign to new array. After performing this operation we will get a blurred image. The blurred image of original image is then bitXOR with Scrambled key image to get encrypted image.

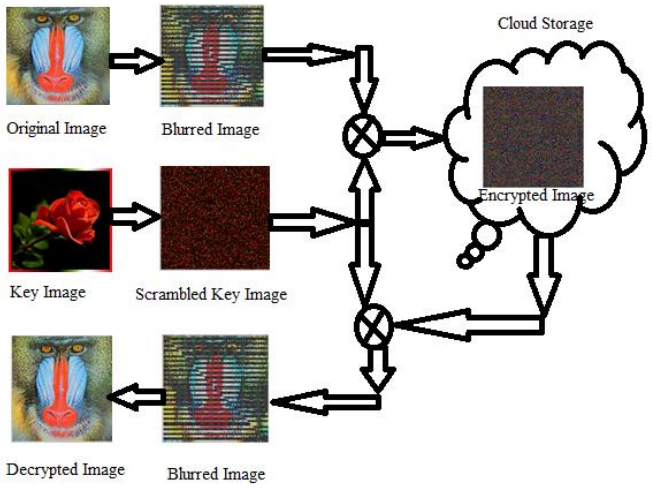

Figure 1: Architecture of Proposed Work

B. Algorithm

Step 1: User input original image and key image
Step 2: Compare the size of key image with original
Step 3: if yes, it go to step 5
Step 4: if no, it will go to step 2
Step 5: Encryption by confusion technique
Step 6: Blurred image
Step 7: scramble the key image
Step 8: XOR Blurred image with scramble key image
Step 9: Encrypted image
Step 10: reverse the algorithm to get the original image

C. Flow chart diagram for encryption and decryption technique

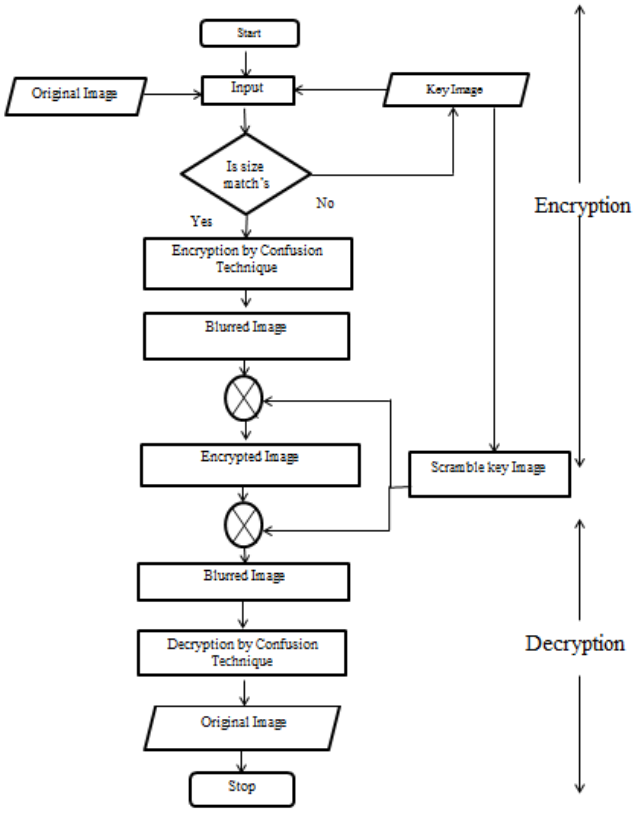

Figure 2: Flow chart of Algorithm

Result

In this section, shows analysis of results where fig 3 is original image 512x512 size, fig 4 shows the histogram of original image, fig 5 shows the encryption of the original image and key image, fig 6 shows histogram of encrypted image, fig 7 shows decrypted image 512x512 size and fig 8 shows histogram of decrypted image.

Figure 3: Original image

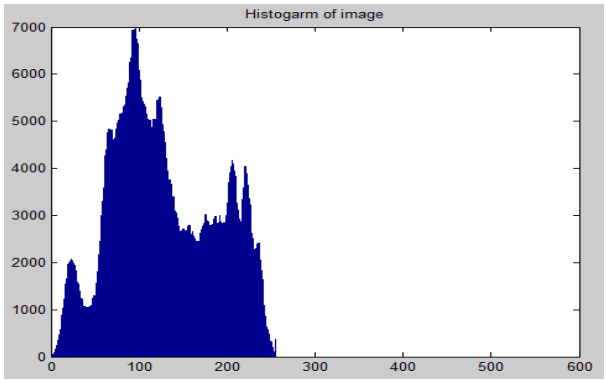

Figure 4: Histogram of original image

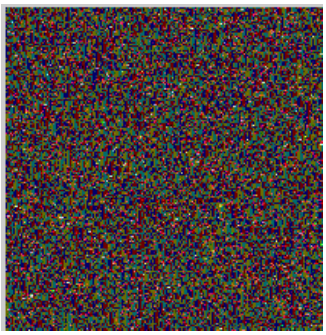

Figure 5: Encrypted image

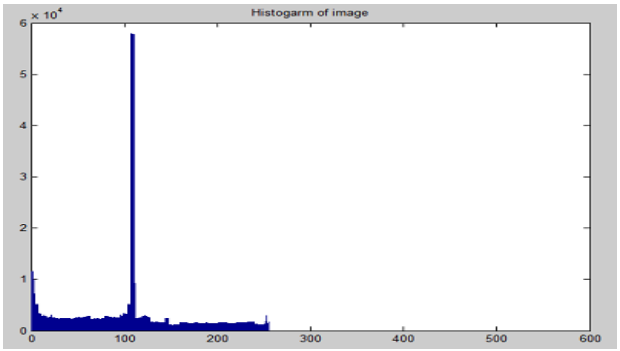

Figure 6: Histogram of encrypted image

Figure 7: Decrypted image

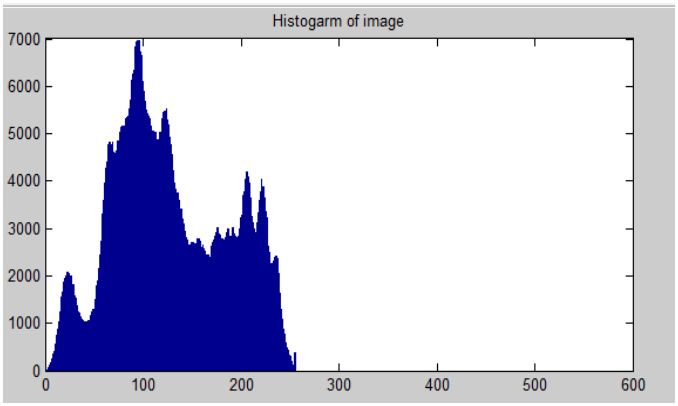

Figure 8: Histogram of Decrypted Image

Table 1: Entropy Information

Image Name	**Entropy of Original Image**	**Entropy of Encrypted Image**	**Entropy of Decrypted Image**
Fruit	7.6698	6.8342	7.6698
Lena	7.7502	6.8959	7.7502
Baboon	7.7624	6.9226	7.7624
Parrot	7.7262	6.8602	7.7262
Rose	4.0369	5.6065	4.0369

According to analysis of result, histogram of original lena fig is compared with histogram of encrypted image fig are different indicating that original image is being protected and cannot retrieved at the time of attack. When comparing with histogram original fig and the decrypted fig where it clearly can be seen that there is no information lost.

According to the TABLE I given, it contains the entropy of original Image and entropy of Decrypted Image when comparing these values in the table indicates that there is no loss of information.

Conclusions

In this paper, a new image encryption technique is proposed based on chaos-based key generation followed by confusion technique and then bitXOR with scramble key image. From our experimental results, we concluded that our schemes with chaos based key generation, key image and confusion technique can resist attack on images in cloud. It is quite safe because the attacker has to find two keys that is chaos based generated key as well as key image to decrypt the image. It is implemented on Matlab 2010. In our future work we will deploy this technique in cloud and try to minimize the complexity of searching the key image for image encryption.

References

[1]. Markets and Markets, "Healthcare cloud computing (clinical, emr, saas, private, public, hybrid) market- global trends, challenges, opportunities & forecasts (2012 - 2017)," July 2012. [Online]. Available: http://www. marketsandmarkets.com/Market- Reports/cloud-computing-healthcare-market-347.html

[2]. C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proceedings of the 41st annual ACM symposium on Theory of computing, 2009, pp. 169–178

[3]. C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," Optics Communications, vol. 285, no. 1, pp. 29 – 37, 2012

[4]. Z. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, pp. 153 – 157, 2005.

[5]. T. Gao and Z. Chen, "A new image encryption algorithm based on hyperchaos," *Physics Letters A*, vol. 372, pp. 394 – 400, 2008.

[6]. Ahmed, Fawad, M. Y. Siyal, and Vali Uddin Abbas. "A perceptually scalable and jpeg compression tolerant image encryption scheme." *Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on*. IEEE, 2010.

[7]. Kester, Q., and Koudjo M. Koumadi. "Cryptographie technique for image encryption based on the RGB pixel displacement." *Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on*. IEEE, 2012.

[8]. Nourian, Arash, and Muthucumaru Maheswaran. "Privacy Enhanced Pixel-Level Image Processing in the Clouds." *Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing*. IEEE Computer Society, 2012.

[9]. Loukhaoukha, Khaled, Makram Nabti, and Khalil Zebbiche. "An efficient image encryption algorithm based on blocks permutation and Rubik's cube principle for iris images." *Systems, Signal Processing and their Applications (WoSSPA), 2013 8th International Workshop on*. IEEE, 2013.

[10]. 8 Jing Qiu and Ping Wang, " Image encryption and authentication scheme", IEEE, Computational Intelligence and Security (CIS), 2011 Seventh International Conference, 3-4 Dec. 2011, 784 – 787

[11]. Narendra K. pareek, Vinod Patidar and K. K. Sud, "Diffusion-Substitution based gray image encryption scheme", Digital Signal Processing, Volume 23, Issue 3, May 2013, pages 894-901.)