Image Symmetric Encryption based on Block Displacement

Samundra Deep
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, 611731, China

Sahil Kohli
Department of Instrumentation Technology
Dayananda Sagar College of Engineering
Bangalore, 560078, India

Javed Ahmed
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, 611731, China

ABSTRACT

The main purpose of this work is the management of security. This will allow users authorization and integrity, accuracy and images security circulating on the Internet. Addition to that, more effort is required for an image-based data in the process of encrypting and decrypting the image. Proposed Architecture facilities for encrypting and decrypting an image using the suitable key and is designed to work for the same purpose. In this article we present a strategy for the new permutations based on a combination of different blocks of pixels and the symmetric encryption algorithm newly developed called "Image Symmetric Encryption Based on Block Displacement". The different blocks of the selected image is formed to change the layout of pixels into an image by the interchanging process, and then using the proposed symmetric encryption Algorithm the processed image will be encrypted.

Keywords

Encryption; Decryption; Security; Image, Cryptography; Algorithm.

1. INTRODUCTION

A Synopsis of Internet Security: From the growth of the Internet, information security and communication has been a prominent issue. Tons of email, file sharing sites, social networks, etc. are transmitting data over the Internet daily. As the number of Internet users rises, the idea of Internet security has found importance. At present, due to the usual movement of digital media transmission of images from around the world, it is important to ensure that they are secure.

A lot of applications, such as military bases, confidential video conference, medical imaging systems, TV cables, private online photo albums, etc demands quick and strong security system for storing and transferring digital images. Several good encryption techniques have been developed for the security needs of these digital technologies. Over the past year, many of the encryption algorithms have been offered formed on different principles. Out of which the encryption technologies constructed on chaos and it is considered to be a practical use, in order to offer better integration of technical speed, higher security, complications, time-wise, and computing power and so forth.

Data management features such as redundancy of data, higher correlation among adjacent pixels of digital images are less sensitive than the text data, i.e., a small transform in the quality of each pixel in the image significantly drop the image quality and the power of open data, etc. Thus, a mixture between adjacent pixels, traditional statistics such as key, AES, DES, RSA, etc. are not considered for real-time encryption when it comes for greater computing and greater power. In order to encrypt the real time image, the ciphers that take lesser amount of time and at the same time without compromising security only those ciphers are preferred.

2. RELATED WORK

Over the past decade, many of the encryption algorithms offered are based on different techniques. Out of these different technologies, encryption technologies based on chaos is considered to be a practical use, in order to offer a good quality of technical speed, higher security, complexity, better time and computing power. Encrypted Images are almost not readable. Therefore, third parties, including server administrators and others have access only to pain text or other information transmitted through the Internet and there are some problems encountered with the image or the encryption process.

Several image encryption algorithms in recent years have been proposed based on the chaotic signals; still it has some issues with the space and the dynamic key distribution. From previous research and other it has conclude that Images and texts are different from each other technically in terms of encryption. It can use conventional cryptosystems encryption directly though it lacks good encryption because of following two reasons. The first one is the size of the image is almost every time much higher than of the text. Thus a conventional cryptosystems require a lot of time for encrypting the image data. And the second is that the decrypted text must equal the original text. But this is not necessarily needed for image data. Because of the human perceptive, an image decrypted with little mutilation is generally tolerable. The decrypted image is not required to be hundred percent original. So at the time of decryption of images it's not necessary that hundred percent original images get. Type of an image is also important factor for encryption/decryption. Presently lots of compressing technique are using to compressed an image , so encryption/decryption are very difficult and time consuming of such type of images.

3. PROPOSED WORK

The purpose of this paper is to provide user with an encryption technique to keep sensitive personal photos from being theft or leak keeping security in mind. The operations follow a number of algorithms in order to ensure the threat and attacks of outsiders to locate and view personal images in personal system or the user wishes to transmit somewhere. In essence, the values of adjacent pixels strongly correlated with natural images, which spread high correlation between pixels and increase the value of entropy; my proposed method is a pure encryption technology. The proposed method is a combination of the two techniques; one is the displacement of pixels horizontally and vertically and the second is a symmetric encryption technique. Basically in this original image will divide into total number of pixels block then these pixels block will be displaced in vertically direction after completing this process resultant image will be displaced in horizontal direction. Finally displaced image will transfer into symmetric encryption process where all the pixels value of image will be read in binary form and it will mix with selected key value by using logical operation in proper way. After completing the whole process resultant image will be called cipher image. Considering entropy and correlation as estimation of security, the output of this would be inferior correlation and a superior value of entropy using the proposed algorithm that will enhance the level of the security of the images encrypted. With the help of displacement process and proposed symmetric encryption/decryption process entropy and correlation can be increase and decrease respectively which is the prime concerned of the proposed research. This encryption technique shortens the reciprocal information increasing the entropy value among the encrypted image variables.

Block Diagram of Proposed Concept: Figure 1 is showing the general block diagram of encryption and decryption, in this an image will pass to the proposed system as an input (only JPG type) then image will go through two step one for displacement another for proposed encryption. And finally cipher image will be produced as an output of the proposed system. Similarly at the time of decryption cipher image will be pass to the proposed system as an input so that the input image goes through a two-stage process designed for encryption and the other is for displacement process. Finally original image is produced by the proposed system. Below shown in figure 2 is the general block diagram of proposed decryption.

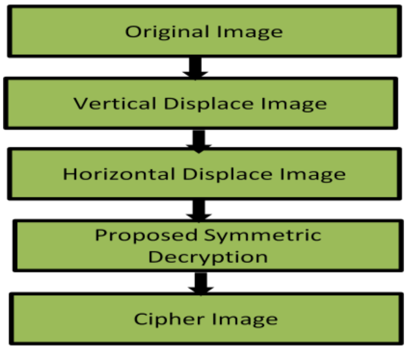

Figure 1: Block Diagram of Proposed Encryption Concept

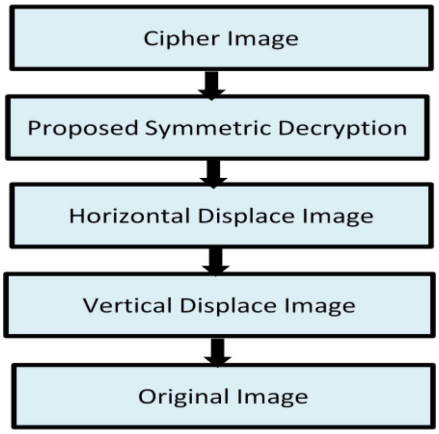

Figure 2: Block Diagram of Proposed Decryption Concept

Proposed Model: The proposed work presents a block-based algorithm and is a combination of image encryption algorithm and image displacement process. The input image is processed into blocks that have been converted into a displaced image using a displacement (vertical and horizontal) algorithm present in future and then the resulted image is then divided into displaced blocks of pixels once again. These pixels block get transfigured into binary value. Likewise proposed encryption algorithm would work with key value. This key value will get transfigured in binary form. Finally key value will use logical operation with Image pixels value. Thus with the proposed algorithm encrypted image is produced.

Algo_Horizontal_Displacement(Image)

```
1.  Image=image (fetch original image)
2.  blockSize=enter block size
3.  rows=image(1); columns=image(2)
4.  horizblock=rows/blocksize;
    vertiblock=columns/blocksize
5.  for i=1 to horizblock
    for j=1 to horizblock
    Move blocks with respect to 1
    End For
    End For
    Start Algo_Vertical_Displacement(Image)
```

Algo_Vertical_Displacement(Image)

```
1.  Image=image (fetch original image)
2.  blockSize=enter block size
3.  rows=image(1); columns=image(2)
4.  horizblock=rows/blocksize;
    vertiblock=columns/blocksize
5.  for i=1 to horizblock
    for j=1 to vertiblock
    Move blocks with respect to 1, 2, 3
    End For
    End For
    Start Perform Encryption(Image,rows,cols)
    End
```

We will compute the security level of the image by using Entropy and Correlation as a measure of security.

Entropy: Entropy is usually used to determine the efficiency of an image, assuming that the image is perfectly represented by its gray level histogram. It also gives an idea of the amount of information is encoded by a compression algorithm[12].

$$H_e = -\sum_{k=0}^{G-1} P(K) \log_2 (P(K))$$

Where:

He: entropy., *G*: input image gray value (0... 255).

P(k): probability of the occurrence of symbol *k*.

Correlation: Digital Image Correlation (DIC) is an analytical technique that compares images of the sample surface during testing to produce a full-field strain maps. Analyzing of the displacement of the pattern is done during the test or experiment. The correlation coefficient r_{ij} can be described as[9]:

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{[n\sum(x^2) - (\sum x)^2 | n\sum(y^2) - (\sum y)^2]}}$$

Where

r: value of correlation,   *n*: the number of pairs of data

∑*xy*: sum of the products of paired data

∑*x*: summation of *x* data,   ∑*y*: summation of *y* data

$\sum x^2$: summation of squared *x* data

$\sum y^2$: sum of squared *y* data

The figure and tables given below show the experimental results done on 4 different images pixels size. The proposed algorithm gets lower correlation and higher entropy of the selected images to conclude better security.

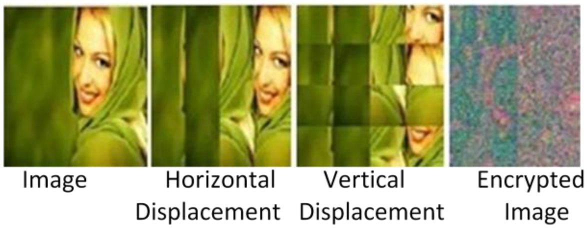

Figure 3: Example of the encrypted Image of proposed Algorithm.

Table 1: Encrypted Images Entropy

S. No.	Images	Entropy
1	Image 1.jpg (200 X 300)	502.345
2	Image 2.jpg (250 X 200)	495.508
3	Image 3.jpg (300 X 200)	509.295
4	Image 4.jpg (200 X 350)	497.645

Table 2: Encrypted Images Entropy Comparison between two different algorithms

S. No.	Images	Existed Algorithm	Proposed Algorithm
1	Image 1.jpg (200 X 300)	LOW	502.345 HIGH
2	Image 2.jpg (250 X 200)	LOW	495.508 HIGH
3	Image 3.jpg (300 X 200)	LOW	509.295 HIGH
4	Image 4.jpg (200 X 350)	LOW	497.645 HIGH

Table 3: Encrypted Images Correlation

S. No.	Images	Correlation
1	Image 1.jpg (200 X 300)	0.0641
2	Image 2.jpg (250 X 200)	0.0537
3	Image 3.jpg (300 X 200)	0.0785
4	Image 4.jpg (200 X 350)	0.0641

Table 4: Encrypted Images Correlation Comparison between two different algorithms

S. No.	Images	Existed Algorithm	Proposed Algorithm
1	Image 1.jpg (200 X 300)	HIGH	0.0641 LOW
2	Image 2.jpg (250 X 200)	HIGH	0.0537 LOW
3	Image 3.jpg (300 X 200)	HIGH	0.0785 LOW
4	Image 4.jpg (200 X 350)	HIGH	0.0641 LOW

4. CONCLUSION

This paper presents an easy yet effective model is proposed for the security of image that used permutation technique which is based on the combination of pixel block interchanging and a newly developed symmetric encryption algorithm. We also conclude that how entropy and correlation can measure the security of the image. From the proposed model it can be seen that the correlation decreases when the proposed displacement process is applied to them before the designed algorithm. Experimental results shows, that correlation is inversely proportional to the number of blocks displaced and entropy is directly proportional number of blocks displaced. In future, we will try to encrypt the images of any size and provide integration of user authentication at the time of image encryption to strengthen the security. We also can combine our proposed algorithm with another encryption technique such as Blowfish Cipher to get better security results. As compared to the results of several standard algorithms, the proposed algorithm produced the lowest correlation and the highest entropy, the best results.

5. REFERENCE

[1] Wu, X., Wong, D., S., LI, Q., “Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion”, Symposium International Computer Science and Computational Technology, pp. 310-315, Dec. 2009.

[2] Najmenik, J., Geisler, W., S., “Optimal Eye Movement Strategies in Visual Search”, Nature 434(3), pp. 387-391, 2005.

[3] S. Changgui, B. Bharat, "An efficient MPEG video encryption a lgor i thm, " Proc e edings of the symposium on reliable distributed systems, IEEE computer society Press, pp. 381-386, 1998.

[4] Jiun-In Guo, Jui-Cheng Yen, “A new mirror-like image encryption algorithm and its VLSI architecture”, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, 2001.

[5] Cimato, S., Santis, A., D., Ferrara, A., L., Masucci, B., “Ideal Contrast Visual Cryptography Schemes with Reversing”, Information Processing Letters, Vol. 93, No. 4, pp. 199-206, February 2005.

[6] Maniccam, S., S., Bourbakis, N., G., ―”Lossless image compression and encryption using SCAN‖, Pattern Recognition” 34, pp. 1229-1245, 2001.

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

[8] Bruce Shnier “Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C”, John Wiley and Sons, Inc., 1996.

[9] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, pp. 1-6, 2003.

[10] Yang, C., N., “New Visual Secrete Sharing Schemes Using Probabilistic Method”, Pattern Recognition Letters Vol. 25, No.4, pp. 481-494, March 2004.

[11] Shyu, S., J., “Efficient Visual Secrete Sharing Scheme for Color Images”, Pattern Recognition, Vol. 39, No. 5, pp. 866-880, 2006.

[12] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[13] Adhikari, A., Dutta, T., K., Roy, B., “A New Black and White Visual Cryptographic Scheme for General Access Structures”, Progress in Cryptography, Vol. 3348, pp. 399-413, 2004.