Data hiding with Pixel scrambling techniques by modified shuffling

Article · January 2014

CITATIONS
0

READS
177

3 authors:

Sourabh Chandra
Calcutta Institute of Technology, Kolkata
37 PUBLICATIONS **80** CITATIONS
SEE PROFILE

Sk Safikul Alam
Jubilant Life Sciences
36 PUBLICATIONS **80** CITATIONS
SEE PROFILE

Debabrata Samanta
Acharya Institutes
11 PUBLICATIONS **16** CITATIONS
SEE PROFILE

International Journal of Information Science and Intelligent System, 3(2): 1-3, 2014

Data hiding with Pixel scrambling techniques by modified shuffling

Sourabh Chandra[1], Sk Safikul Alam[2], Debabrata Samanta[3]

[1] *Asst Professor, CSE Department, Calcutta Institute of Technology, West Bengal, India*
[2] *Asst Professor, CSE Department, Calcutta Institute of Technology, West Bengal, India*
[3] *Asst. Professor, MCA Department, Acharya Institute of Technology, Bangalore, India*

Received:; Accepted:

Abstract

Image scrambling is an effective method for providing image security. The basic idea of scrambling is to change the image pixel positions through matrix transform to achieve the visual effect of disorder. Cellular automata can be successfully applied for this purpose. This paper presents digital image scrambling based on modified shuffling. The method proposed is a simple but powerful technique. The method uses R-Prime Shuffle to encrypt the image. It makes use of two different R-Prime numbers for rows and columns which make it more robust to decryption.The proposed algorithm transforms drastically the statistical characteristic of original image information, so, it increases the difficulty of an unauthorized individual to break the encryption. The simulation results and the performance analysis show that the algorithm has large secret-key space, high security, fast scrambling speed and strong robustness.

Keywords: First word; Second word; Third word; Fourth word

1. Introduction

In Finding effective ways to protect image data is challenging even with the most advanced technology and trained professionals. The increasing number of information-security-related incidents and organized crimes means that securing information is becoming a major issue in the current information-based economy. This has forced academicians, industrialists and researchers to focus on the protection of images during transmission. To secure information, many research directions have been suggested in the past few decades.

Thus, in the present paper work, a chaotic-based image scrambling encryption method that can be combined with JPEG compression technique is proposed.

2. Related Work

Image scrambling is an important technique in digital image encryption and digital image watermarking. Image scrambling is commonly used in image encryption, and is also used in watermarking to make the image statistically undetectable. It is a field that has drawn

much attention in the latest years. The main aim of image scrambling is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. Now, the mainly used three kind of image scrambling types are scrambling in the space domain, scrambling in the frequency domain, and scrambling in the color or grey domain.

The image scrambling algorithm using parameter based M-sequence transforms. The data of a 2-D image is a 2-D matrix while the data of a 3-component color image is consisted of three 2-D Matrices, one matrix for each of the 3 different color planes of an image. Choosing the 3-D M-sequence transform to scramble the color images is a more efficient way than selecting 2-D M-sequence transform. Similarly, the 2-D M-sequence transform is more efficient for scrambling the 2-D images in one step such as grayscale images, binary images, medical images, and so on. The image scrambling algorithm is shown as Figure 1. The 2-D or 3-D transform will be chosen based on the characteristics of the image data. If the image is a 2-D image, the 2-D M-sequence transform will be chosen to scramble the image data. Otherwise, the 3-D transform will be selected. The row and column coefficient matrices should be calculated by choosing the security keys: the shift parameter r and the distance parameter p. The scrambled image can be generated by applying the 2-D/3-D M-sequence transform to the original image at one time. The authorized users should be provided the security keys to reconstruct the original image in their inverse process. The security keys will be used to calculate the inverse row and column coefficient matrices. The inverse 2-D M-sequence transform will be selected if the image data is a 2-D matrix. On the other hand, the inverse 3-D transform will be used to decode the scrambled image data. The reconstructed images can be obtained by applying the inverse transform to the scrambled image.

3. Proposed Algorithms

The process of proposed algorithm that combines encryption and compression is given in Figure1. This process is divided into three steps,

(i)Color Space Conversion
(ii) Key Generator and Scrambling Algorithm
(iii) JPEG Compression

The color space of the image is first converted to YUV color space .The two most widely used color spaces for storing digital images are RGB color space and YUV color space.

A. Scrambling Algorithm

The proposed image encryption algorithm consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete states variables of chaotic maps. The purpose of scrambling is to transform, a meaningful image into a meaningless, disordered and unsystematic image to obscure real meaning of image. A secret scrambling increases the computational complexity of potential chosen-plaintext attack,

thereby making cryptanalysis of image encryption much more complicated. The result of scrambling algorithm is shown in Figure 1.

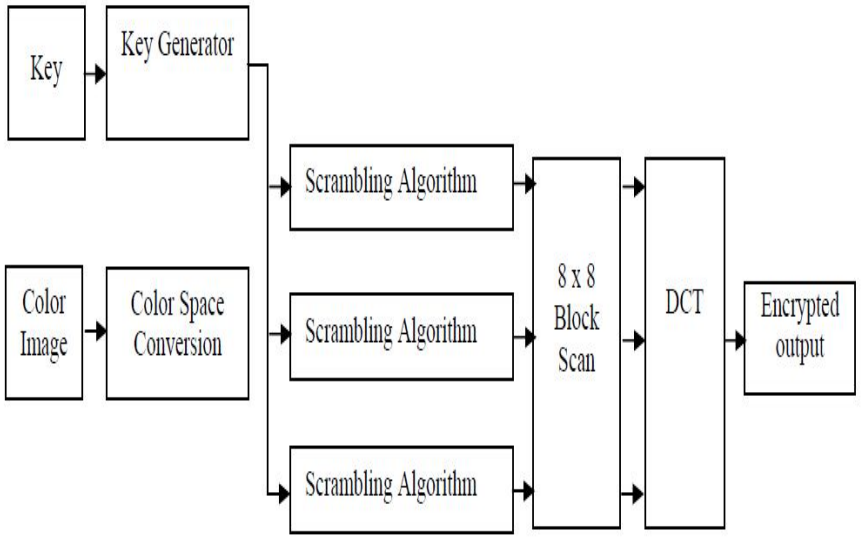

Figure 1: Proposed Encryption Scheme for Picture and Graphics Block

4. Experimental Result

In order to test the performance of the developed scrambling method, this paper used MATLAB to simulate this algorithm. We consider gray image of 256×256, a gray image of 144 × 256 and a color image of 256 × 256 as experimental images.

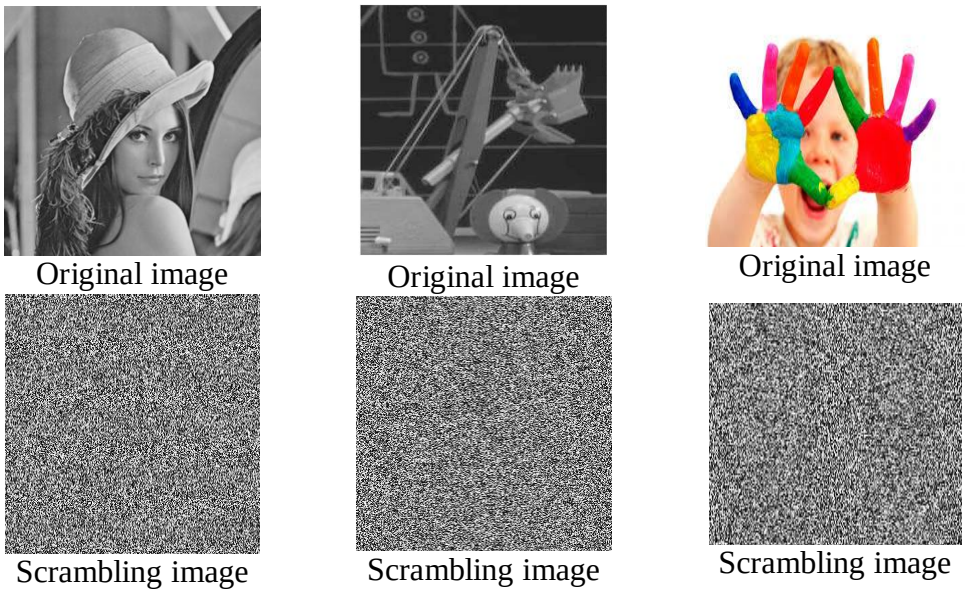

Figure 2: Result of developed method

A. Encryption

The method used for Encryption is as follows
1) Read the image
2) Convert it to grayscale
3) Based on the Size of the Image (MXN), find out all the Relative Prime Numbers and save them in a set S
4) Using set S to find the correlation of the First row with remaining rows (positions w.r.t elements present in the set).
5) Consider the lowest correlation as the key to shuffle the rows in the image
6) continue till all the positions in the image are considered
7) Save the Relative Primes Number as a key considered for Row Shuffling

B. Decryption

1) Use the Saved key for Row and Column Shuffling to get the Original Image back
2) Use the column Relative Prime and rearrange the columns, this will give row shuffled image
3) Using this row shuffled image and the key for row relative prime rearrange the rows which will give you Original Image back.
4) continue till all the positions in the image are rearranged

5. Simulation Experiment and Analysis

The system was evaluated using various aspects like Compression Ratio, and Peak Signal to Noise Ratio (PSNR).

C. Performance Metrics

The performance of the proposed models was evaluated using different parameters like Average Moving Distance of
Scrambling**,** Hamming Correlativity and Peak Signal to Noise Ratio. One of the objectives of the proposed compression models is to maintain the visual quality of the decompressed image. The quality of the decompressed image was ascertained by using the quality metric Peak Signal to Noise Ratio (PSNR).

D. *Average* Moving Distance of Scrambling

The average moving distance of scrambling is defined as Equation (1).

$$\|D\|_2 = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \sqrt{(w-i)^2 + (v-j)^2} \qquad (1)$$

where M and N is the dimension of the image, i, j are coordinates of original and w and v are coordinates of encrypted image. The larger the Average distance ratio the less is the relation between the original and encrypted image. Table I shows the average moving distance of scrambling obtained by the proposed algorithm while given with 256 x 256 images.

E. Peak Signal to Noise Ratio

In the present paper work, the encryption algorithm is combined with JPEG compression technique, so that it will provide an efficiency way for transmitting images. Several experiments were conducted to verify the quality of the image after decryption. The quality of the image was ascertained using the PSNR metric and is tabulated in Table III for the two selected images.

Image Used	**PSNR**
Image 1	43.83
Image 3	41.59
Image 3	46.28

Table I: PSNR after decryption

The high value obtained proves that the quality of the image after decryption and decompression is good and can be considered by many transmission applications.

F. Analysis of Histogram

Carry out analysis through the gray histogram of the image before and after encryption. From the Figure 3 it can be seen that the distribution of primitive image pixel gray values is concentrated on some values, while the pixel gray values after the encryption are scattering in the entire pixel value space. Accordingly it indicates that this encryption method has very good characteristics of gray evenly distribution. Thereby, it can fight against certain degree of statistic analysis attack.

To quantify the performance of the proposed algorithm, we computed the signal-to-noise ratio (SNR) index for each original image. We computed SNR for the original images in the decrypted images for two experiments, respectively. For comparison, we also computed SNR for the original images in the encrypted images.

G. Speed Analysis

The execution time can demonstrate how efficiently the encryption algorithms encrypt image. This feature is designed to show whether the encryption algorithm can meet the requirements of low computation and high processing speed in real-time applications. Table 2 gives the execution time. The result was measured on a computer running the Windows 7 operating system with 2GB memory and with a CPU using Intel(R) core(TM)2 Duo CPU T6600. The time of encryption process was measured when the Logistic sequence was applied individually to image. The results has shown that there is a familiar relation with the size of images and the running time of this method is short, encryption and decryption time can meet the requirements of the normal operation.

Process execution time(s)	**Lenna (256×256)**	**Image (144X256)**	**RGB (256×256)**
Encryption	0.005	0.0878	0.1225
Decryption	0.024	0.0929	0.0974

Table 2: Execution Time Statistics

6. Conclusion

Simulation analysis shows that the encryption algorithm has characters of strong keys, better effect and fast. Experimental results demonstrate that the proposed algorithm successfully achieves image scrambling, showing effective hiding ability for image information with significant advantages:

• Easy to operate.
• Small computation burden.
• Strong adaptability. It is applicable for various types and sizes of image scrambling.
• Strong applicability. It possesses perfect confusion properties and it can resist the various attacks. Experiments conducted with natural images show that the proposed algorithm is strong in providing security and is also very fast.

References

[1] J. V. Neumann, ―Theory of self-reproducing automata,‖ University of Illinois Press, 1966.
[2] S. Wolfram, ―Computation theory of cellular automata‖. Commun. Math. Phys., vol. 96, pp. 15-57, 1984.
[3] P. Andreas and U. Andreas, ―Image and video encryption,‖ Proc of Advances in Information Security Series, Springer Press, 15, 2005.
[4] F. Maleki, A. Mohades, S. Hashemi, and M. Shiri ―An image encryption system by cellular automata with memory,‖ Proc. of Third International Conference on Availability, Reliability and Security, Barcelona, 2008, pp.1266-1271.
[5] X. Desheng and X. Yueshan, ―Digital image scrambling based on Josephus traversing,‖ Computer Engineering and Applications, vol. 10, 2005.
[6] G. Ye, X. Huang, and C. Zhu, ―Image encryption algorithm of double scrambling based on ASCII code of matrix element,‖ Proc. of International Conference on Computational Intelligence and Security, pp 843-847, 2007.
[7] Shujun Li , Xuan Zheng, "On the Security of an Image Encryption Method" in Proc International Conference on Image Processing ICIP'2002, pp II-925 - II-928 vol.2 IEEE
[8] Chenghang Yu, Baojun Zhang, Xiang Ruan, "The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption" in Proc Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2011. pp 390-395.
[9] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", in Proc International Conference on Electronics and Information Engineering (ICEIE 2010), Volume 1, pp V1-141-145.
[10] Ravankar,A.A., Sedukhin, S.G., "Image Scrambling Based on a New Linear Transform", in Proc International Conference on Multimedia Technology (ICMT), 2011
[11] Jiancheng Zou, Rabab K. Ward, Dongxu Qi, "A New Digital Image Scrambling Method based on Fibonacci Numbers" ,in Proc. IEEE ISCAS 2004, vol. III, pp. 965 – 968.
[12] W. Zou, J. Huang and C. Zhou, "Digital Image Scrambling Technology Based On Two Dimension Fibonacci Transformation And Its Periodicity", Third International symposium on Information Science and Engineering, (2010) December 24-26, Shanghai: China.