International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 512 – 515

Review on Color Image Encryption Algorithm based on Pseudorandom Number Key

Miss. K. S. Butle
Department of EXTC
B. D. College of Engineering,
Sevagram, India
Email:kalyani.butle517@gmail.com

Prof. R. M. Mandavgane
Department of EXTC
B. D. College of Engineering,
Sevagram, India
Email: rmmandavgane@rediffmail.com

Prof. D. M. Khatri
Department of EXTC
B. D. College of Engineering,
Sevagram, India
Email:deepali.85@rediffmail.com

Abstract: In secure communication, image encryption schemes transform clear images into unintelligible others. The fundamental techniques used to encrypt a block of pixels are substitution and permutation. In recent years focuses on designing of highly robust encryption schemes (i.e., which provide good confusion and diffusion properties, to ensure desired security factor), either using peculiar pixel shuffling methods, or using innovative digital chaos-based ciphers, or by making justified compositions between these different pixel shuffling and ciphering techniques. Almost some encryption schemes based on permutation had already been found insecure against the cipher text-only and known/chosen-plaintext attacks, due to the high information redundancy, and it is quite understandable since the secret permutations can be recovered by comparing the plaintexts and the permuted cipher texts. Generally, chaos-based image encryption algorithms are used more often than others but require high computational cost. Moreover, a chaos system is defined on real numbers while the cryptosystems are defined on finite sets of integers. Furthermore, spatial domain scrambling has defect that the statistical characteristics of image are not changed after scrambling. Therefore, it is not secure to perform scrambling in spatial domain. The image encryption methods based on frequency domain encrypt/decrypt the images by modifying the image frequencies. One can recover the original plain image exactly via a reverse process.

*****

1. Introduction

Modern telecommunications technologies facilitate to transmit large amount of digital information over public networks. It is mandatory task to protect information against unauthorized access, usage, disruption and destruction. In the past years, many encryption methods have been proposed, for example DES, IDEA, RSA etc. However, these conventional encryption algorithms are not suitable for digital images due to inherent features of image data like bulk data capacity and high redundancy.

Encryption has long been used to securely save and transfer data and protect it from possible attacks. With the rapid increase in transferring images over the internet and mobile phones, efficient and strong image encryption techniques are needed. Cryptography and steganography are two different approaches for achieving this privacy. In cryptography, original data is coded into unreadable ciphered form before storing or transmitting it. On the other hand, steganography embeds the original data into a cover media, such as images, audio or video, to hide its existence. In other words, steganography performs data hiding such that no one other than the intended recipient knows of its existence. This is in contrast to cryptography, where the existence of the data is not hidden but its content is obscured. Digital cryptosystems are typically divided into two generic types according to the key distribution: symmetric-key and asymmetric-key. Symmetric-key cryptosystems use the same secret key for encryption as well as decryption. Because of their efficiency, they are appropriate for handling large amounts of data at high speed. The key length of symmetric ciphers usually ranges from 128 to 256 bits. With respect to the encryption algorithm, cryptosystems are divided into block and stream ciphers. Block ciphers encrypt the original message by grouping the symbols in blocks such that each block is always encrypted / decrypted in the same way. Stream ciphers generate a pseudorandom stream of symbols using a deterministic public algorithm governed by a secret key. The message is mixed with this sequence, usually through modulo 2 sum (exclusive or, XOR), resulting in the ciphered message.

The image encryption system uses fractal images as a highly variant source for encrypting other images. Although the concept of fractals includes a wide class of objects, many of the most popular fractal images can be obtained through IFS. IFS have received a lot of attention because of their appealing combination of conceptual simplicity, computational efficiency and great ability to reproduce natural formations and complex phenomena. There are miscellaneous programs, which are freely available on the internet, for generating and rendering IFS fractals. In general, the process of generating a fractal can be simplified into three stages. In the first stage, all initializations take place. In the second stage, the iteration formula is applied repeatedly under a condition of termination. Finally, the third stage performs post-processing on the resulting vector (pixel rendering). In this system, each fractal can, first, be shifted in both horizontal and/or vertical directions. Then, some selected fractals are XORed with the source image to produce a modified image. To strengthen the encryption system, delay and multiplexing blocks are added to help in

making the encrypted image look random. The delay block serves as the memory of the encryption system, which utilizes the previous encryption result. The multiplexing block selects which color channels of the delayed and modified images are XORed together to produce the final encrypted image.

Chaos based encryption is one of these efficient techniques due to its unique properties, such as the sensitive dependence on initial conditions and system parameters i.e. a tiny change of the initial input values leads to a great different of the output, unpredictable and its random-like properties, which are satisfied the requirements of cryptography. Especially, chaotic systems based image ciphers are very popular with the researchers as a good solution to image encryption in the past few years

To evaluate how each system block contributes to the encryption process, we start by using only one fractal image and analyzing the encryption results. After that, the system is examined using multi-fractal images and the analysis results are given. The encrypted images are analyzed using correlation coefficients, differential attack measures, histogram distributions and NIST statistical test suite.

The brief overview of four commonly used evaluation criteria for encryption system is as follows.

- *Image Pixel Correlation:*

Image pixels are highly correlated to each other and, hence, one of the encryption targets is to make the correlation coefficients for horizontal, vertical and diagonal pixels very small.

- *Peak Signal Noise Ratio:*

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image encryption quality. The MSE represents the cumulative squared error between the encrypted and the original image, whereas PSNR represents a measure of the peak error.

- *Entropy Analysis:*

Entropy is a measure of the predictability of a random source. Owing to the high correlation between adjacent pixels, image data is predictable and consequently has low entropy. Ciphered image data on the other hand should appear as random noise to avoid any information leakage. For a binary source producing 2^8 symbols of equal probabilities and each symbol is 8 bits long.

- *Pixels change rate (NPCR)* :

NPCR concentrates on the absolute number of pixels which changes value in differential attacks.

- *Unified average changing intensity (UACI):*

UACI focuses on the averaged difference between two paired cipher text images.

2. Literature Review

In this paper [1], design of a stream-cipher algorithm based on one-time keys and robust chaotic maps, in order to get high security and improve the dynamical degradation. We utilized the piecewise linear chaotic map as the generator of a pseudo-random key stream sequence. The initial conditions were generated by the true random number generators, the MD5 of the mouse positions. When the collision of MD5 had been found, we combined the algorithm with the traditional cycle encryption to ensure higher security. The ciphered image is robust against noise, and makes known attack unfeasible. It is suitable for application in color image encryption.

This paper [2] study introduces a novel image encryption system based on diffusion and confusion processes in which the image information is hidden inside the complex details of fractal images. A simplified encryption technique is, first, presented using a single-fractal image and statistical analysis is performed. A general encryption system utilizing multiple fractal images is, then, introduced to improve the performance and increase the encryption key up to hundreds of bits. This improvement is achieved through several parameters: feedback delay, multiplexing and independent horizontal or vertical shifts. The effect of each parameter is studied separately and, then, they are combined to illustrate their influence on the encryption quality. The encryption quality is evaluated using different analysis techniques such as correlation coefficients, differential attack measures, histogram distributions, key sensitivity analysis and the National Institute of Standards and Technology (NIST) statistical test suite. The obtained results show great potential compared to other techniques.

In this paper [3], an image encryption algorithm with the architecture of combining permutation and diffusion is proposed. The plain-image is first partitioned into blocks of 8×8 pixels. A spatiotemporal chaotic system is then employed to generate the pseudorandom sequence used for diffusing and shuffling the blocks. The objectives of this new design include: (i) to efficiently extract good pseudorandom sequences from a spatiotemporal chaotic system and (ii) to simultaneously perform permutation and diffusion operations for fast encryption. As a result, the image needs to be scanned only once in each encryption round, while the other existing algorithms separate the permutation and diffusion stages therefore require at least two image-scanning processes. The other technique is an effective generation of pseudorandom numbers from the NCML by some traditional cryptographic operations. It avoids time-consuming operations such as multiplication and conversion from floating points to integers, consequently a higher encryption speed is obtained. Upon completion of the design, both theoretical analyses and experimental tests have been

carried out, both confirming that the new cipher possesses high security and fast encryption speed. In conclusion, therefore, the new cipher indeed has excellent potential for practical image encryption applications.

In this paper [4], a DWT based lossless encryption algorithm for color images by using CML is proposed. In our work, the DWT Haar transform is employed. We first convert the plain-image from the spatial domain to the frequency domain by DWT Haar transform. Then key streams are generated from CML and the plain-image, and used to scramble the image subbands. The resulting cipher-image is obtained via transforming the image frequencies back to the spatial domain. The experimental results show that the proposed encryption scheme is a lossless encryption algorithm and has high security. The proposed encryption algorithm is robust towards cryptanalysis and also fast making it suitable for real-time encryption and transmission.

In this paper [5], we propose a new method to develop secure image-encryption techniques using a logistics –based encryption algorithm. In this technique, a Haar wavelet transform was used to decompose the image and decorrelate its pixels into averaging and differencing components. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. The remaining components (the differencing components) are compressed using a wavelet transform. Many test images are used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provides an efficient and secure approach to real-time image encryption and transmission.

In this paper [6], we proposed a new combined chaotic system using two traditional chaotic maps: the Logistic map and Sine map. The bifurcation diagram and trajectory of the proposed chaotic map demonstrated its better random-like property and high sensitivity to its initial values and parameters. Moreover, the control parameter has a larger chaotic interval compare with traditional chaotic maps. This ensures the proposed chaotic system more suitable for cryptography applications.

3. Overall Analysis of Research Work

Haar wavelet transform was used to decompose the image and decorrelate its pixels into averaging and differencing components. Many test images are used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provides an efficient and secure approach to real-time image encryption and transmission. Table 1 shows the comparative table of parameters in encryption. Proposed color image encryption algorithm using Daubechies wavelet transform and logistics chaotic maps using pseudo random number generator would result in batter encryption parameters.

4. Conclusion

In many papers proposes a chaotic system using two traditional chaotic maps: the Logistic map and Sine map or combination of both. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. In some papers encryption system with two major parts, chaotic pixels substitution (in order to achieve desired diffusion factor) and chaotic maps based, pixels permutation (in order to achieve desired confusion factor). The performance assessment tests attest that the proposed image encryption scheme is fast and highly secure. Although a much smaller key space is used, but still large enough to face against exhaustive attack, with a smaller key size, the proposed encryption scheme presents better results, compared to those of previously proposed ones.

Table 1 Comparative Table

Reference	[1]	[2]	[3]	[4]	[5]
Plane Image Horizontal CC	0.985	0.97	0.98648	0.967	-
Plane Image Vertical CC	0.968	0.96	0.98863	0.971	-
Plane Image Diagonal CC	0.966	0.93	0.97762	0.942	-
Cipher Image Horizontal CC	0.031	0.0647	0.00070	0.485	-
Cipher Image Vertical CC	0.096	0.0006	0.00216	0.492	-
Cipher Image Diagonal CC	0.036	0.000	0.01488	0.487	-
PSNR	-	-	-	-	71.0
Entropy	7.985	7.59	-	7.62	7.9
NPCR (Max)	99.6	99.7	97.5	-	-
UACI (Max)	33.6	33.4	32.7	-	-

References

[1] Liu Hongjuna, Wang Xingyuana, “Color image encryption based on one-time keys and robust chaotic maps”, in Elsevier Journal Computers and Mathematics with Applications, vol 59, 2010, pp 3320 – 3327.

[2] Salwa Kamal Abd-El-Hafiz, Ahmed G. Radwan, Sherif H. Abdel Haleem, Mohamed L. Barakat, "A fractal-based image encryption system", in IEEE Transaction on Image Processing, vol. 8, issue 12, 2013, pp. 742 – 752.

[3] Yong Wang, et al, "A new chaos-based fast image encryption algorithm", in Elsevier Journal of Applied Soft Computing, vol. 11, 2011, pp 514 - 522.

[4] Xiangjun Wu, Zefan Wang, "A new DWT-based Lossless Chaotic Encryption Scheme for Color Images", in IEEE International Conference on Computer and Computational Sciences, 2015.

[5] Nidhi Sethi, Deepika Sharma, "A New Cryptology Approach for Image Encryption", in 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012.

[6] C.L. Philip Chen, Tong Zhang, Yicong Zhou, "Image Encryption Algorithm Based on A New Combined Chaotic System", in IEEE International Conference on Systems, Man, and Cybernetics, 2012.

[7] C. Samson and V. Sastry, "A novel image encryption supported by compression using multilevel wavelet transform," Int. J. Adv. Comput. Sci. Appl., vol. 3, pp.178–183, September 2012.

[8] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image encryption using DCT and stream cipher," Eur. J. Sci. Res., vol. 32, pp.47–57, January 2009.

[9] S. Tedmori and N. Al-Najdawi, "Lossless image cryptography algorithm based on discrete cosine transform," Int. Arab J. Inform. Technol., vol. 9, pp. 471–478, May 2012.

[10] L. Sui, M. Xin, A. Tian, and H. Jin, "Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain," Opt. Lasers Eng., vol. 51, pp.1297–1309, December 2013.

[11] S. Tedmori and Nijad Al-Najdawi, "Image cryptographic algorithm based on the Haar wavelet transform," Inform. Sci., vol. 269, pp.21– 34, June 2014

[12] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," Commun. Nonlinear Sci. Numer. Simulat, vol. 20, pp.447–460, February 2015.