An Image Encryption Technique to Remove the Drawback of the One-Dimensional Scrambling Method of Image Encryption

Mohit Kumar
Research Scholar
Amity University Haryana
India

Anju Chahal
Research Scholar
Amity University Haryana
India

ABSTRACT

Images are gaining popularity in communication, entertainment and business etc. Some images can have confidential information so the security of these confidential images is a crucial issue. There is the image encryption technique that uses a one-dimensional random scrambling and provides security to secret images. The drawback of this technique is that it does not produce different histogram from the histogram of original image even after encryption procedure and this unchanged histogram reveals useful information about the original image. In this paper, an image encryption method is proposed that eliminates this drawback and provides better security than algorithm that uses one dimensional random scrambling.

General Terms

Cryptography, image security, image processing.

Keywords

Confusion, decrypted image, diffusion, encrypted image, histogram, image encryption, scrambling, substitution

1. INTRODUCTION

Internet and information technology are developing rapidly. People use multimedia for communication as well as for other purpose like entertainment and business etc. There is a major role of images in communication and entertainment. When a user transfer an image over an unsecured communication network, then there is always a threat to get accessed this image illegally. So a need of a technique arises that can prevent illegal access to a confidential information.

Encryption is an excellent way to provide security to images. Encryption is a process that encodes a plain image into a coded form that is difficult to understand. A secret key is used in an enciphering process to make it secure. A key is also used in deciphering procedure. Keys that are used in encryption and decryption may be same or different as per requirement. If the same key is used in encoding and decoding, then it is called symmetric key encryption otherwise it is called asymmetric key encryption [1]. A figure 1 illustrates the basic model of making an image secure. Figure 2 show a plain image and after applying encryption process it is converted into an encrypted or encoded image that is difficult to understand. Figure 3 represents the encrypted image. A receiver can decode this encrypted image by applying decryption process that is generally reversed process of encryption process. Figure 4 demonstrates the decrypted or decoded image that represents original information.

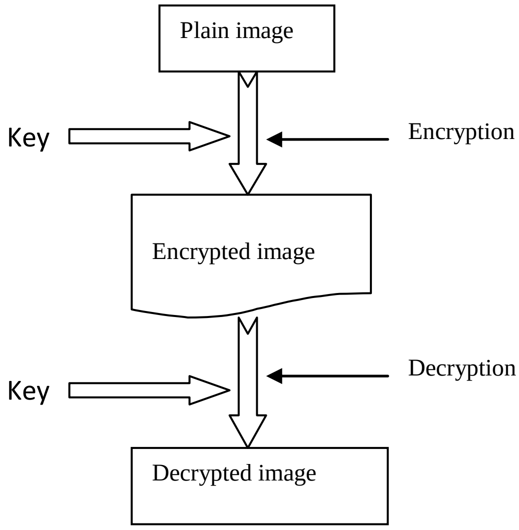

Fig 1: Block diagram of making an image secure

Fig 2: Plain image

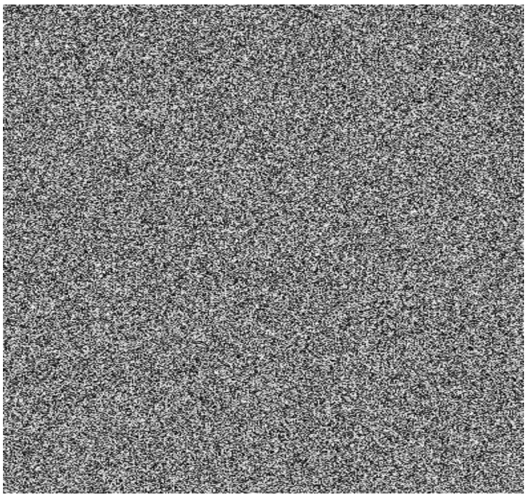

Fig 3: Encrypted image

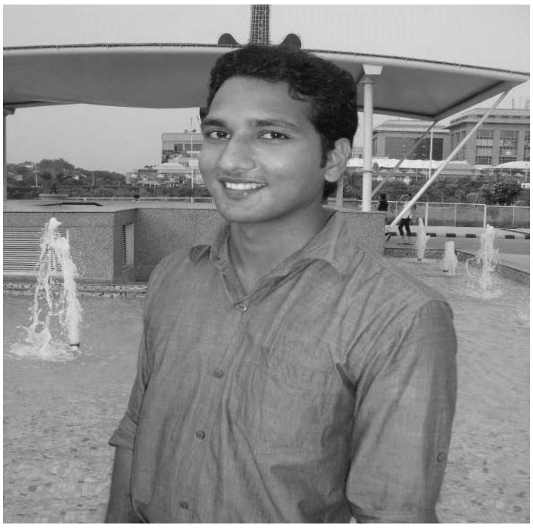

Fig 4: Decrypted image

There are various data encryption algorithms, for example IDEA, AES, DES and RSA. However, these techniques are capable to encrypt text data nevertheless deficient in image encryption [2]. Images are different from text data due to bulky data, high redundancy and strong correlation between pixels [3, 4, 5, 6]. So there is a need of encryption technique that is suitable for images [3, 4, 5].

This paper has an image encryption algorithm that is based on scrambling and substitution of pixels.

2. EXISTING ALGORITHM AND ITS DRAWBACK

Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue [7] have proposed a one-dimensional random scrambling based algorithm. At the first step, this algorithm converts a two-dimensional image into the one-dimensional vector and then operates the one-dimensional random shuffling [7]. Thereafter, the proposed algorithm performs an anti transformation on this scrambled vector to generate an encipher image. Consequently, the suggested scheme does not need the iterative computation, since, one or two executions are sufficient for the best result. Figure 5 shows an original image; after operating the first iteration of the procedure, algorithm produces an encoded image, which is illustrated in figure 6. After operating 15 rounds; a usable encoded image is produced, which is represented in figure 7. Moreover, figure 8 and figure 9 show the histogram of the original image and encrypted image respectively.

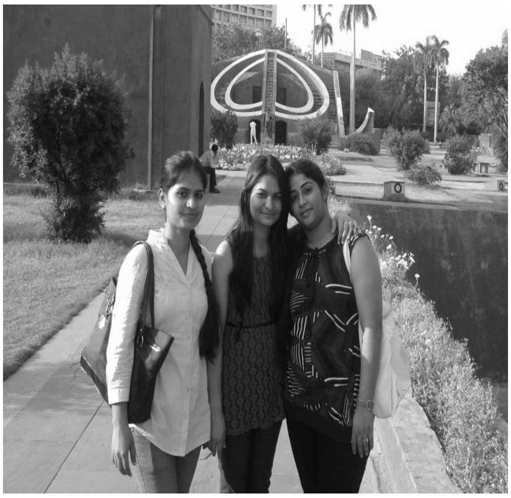

Fig 5: Original image

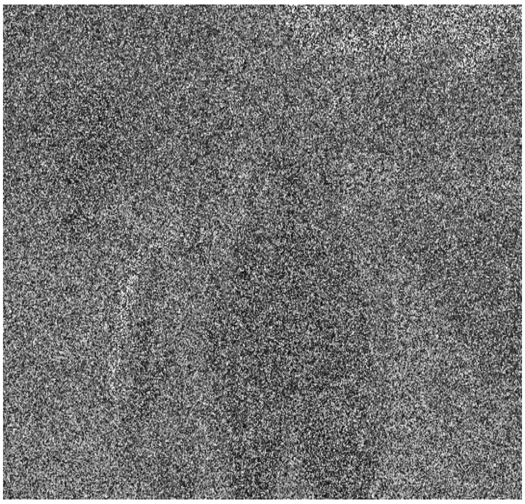

Fig 6: Encrypted image at iteration 1

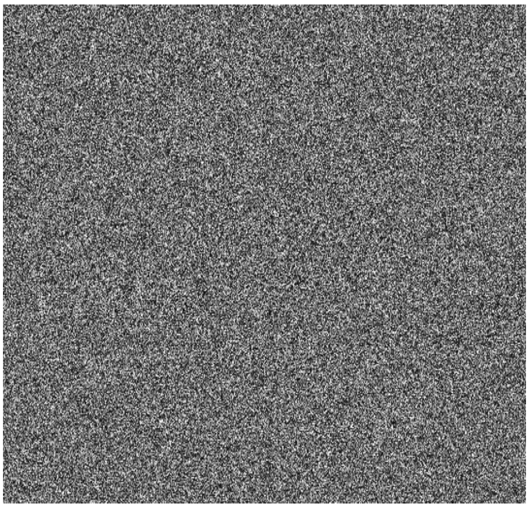

Fig 7: Encrypted image at 15 iterations

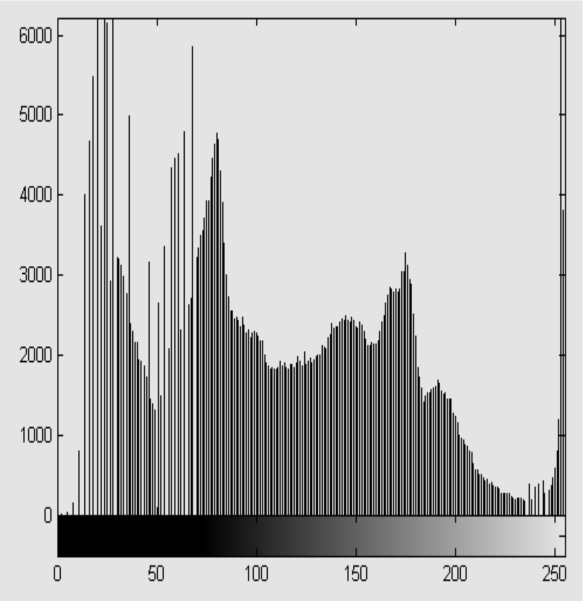

Fig 8: Histogram of original image

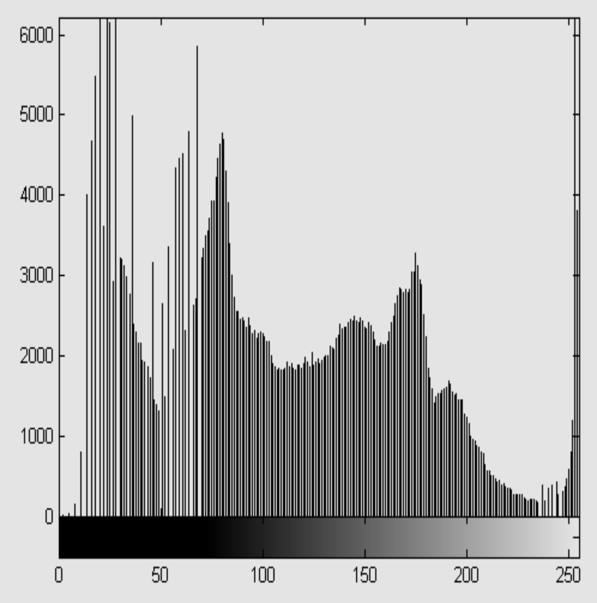

Fig 9: Histogram of encrypted image after 15 iterations

This algorithm has a drawback that it is unable to produce a different histogram from the histogram of the original image. The histogram of original image and encrypted image are same. It means that this algorithm does not satisfy confusion property. An image encryption algorithm should show the both confusion and diffusion in image to provide effective security.

This technique uses only scrambling process that creates only diffusion and only diffusion is not sufficient for effective security. The encrypted image has an unchanged histogram so opponent can retrieve the major information about frequency distribution of pixels in the image. Consequently, adversary is able to produce original image easily with the information of frequency distribution.

3. PROPOSED TECHNIQUE

The proposed method is able to eliminate the drawback of the algorithm imparted by Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue that uses only scrambling process. The suggested technique uses scrambling with a substitution to satisfy Shannon’s confusion and diffusion properties. This technique works in two phases: scrambling phase and substitution phase. Furthermore, this procedure uses a key that has 400 bits.

3.1 Scrambling

This phase has following steps

Step 1: apply interchanging operation among rows with the help of key.

Step 2: apply interchanging operation among columns with the help of key.

Step 3: operate circular rotation on all rows with the help of key.

Step 4: operate circular rotation on all columns with the help of key.

Step 5: end of scrambling process.

Step 6: A scrambled image is produced and this image will enter in substitution phase.

3.2 Substitution

This phase has following steps

Step 1: convert image matrix to one-dimensional array.

Step 2: pick 50 pixels in sequence and convert into bits.

Step 3: apply the XOR operation on these bits with a key of 400 bits.

Step 4: apply a circular shift operation on the result of step 3 with the help of key.

Step 5: take the complement of key

Step 6: apply again XOR operation on the result of step 4 and the complement of key.

Step 7: decompose the resulting 400 bits of step 6 into 50 segments. Each segment will have 8 bits.

Step 8: convert each segment to equivalent decimal number. These decimal numbers are encrypted pixels.

Step 9: replace these encrypted pixels with the old pixels in one-dimensional array.

Step 10: pick next 50 pixels and repeat step from 3 to 9.

Step 11: if 50 pixels are not available for encryption in the last, then pick the rest pixels and repeat step from 3 to 9. But this time key will have the number of bits that will be equal to number of rest pixels multiplied by 8.

Step 12: convert one-dimensional array into two-dimensional matrix having the same dimension as the original image.

Step 13 end of substitution process. The resultant matrix is encrypted image.

Figure 10 illustrates the block diagram of the proposed image encryption algorithm.

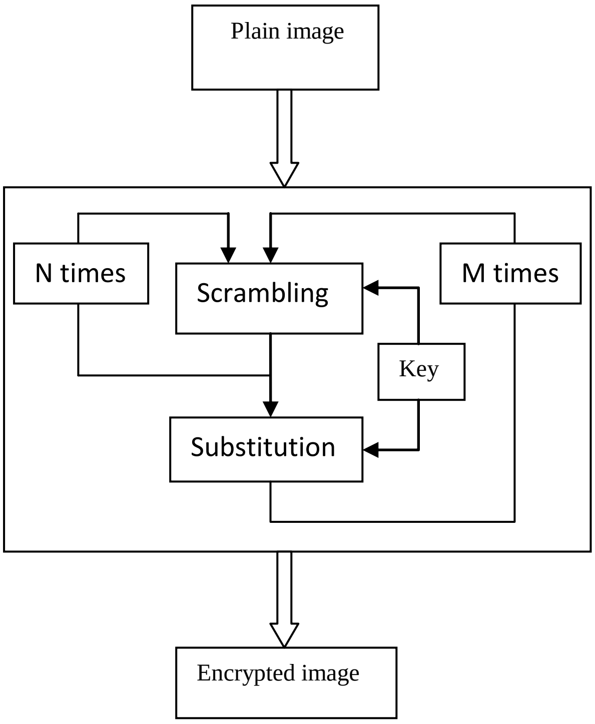

Fig 10: Block diagram of proposed technique

4. EXPERIMENTAL RESULT OF PROPOSED TECHNIQUE

The proposed algorithm encrypts the plain image that is shown in figure 11. Figure 12 represents an encrypted image that is retrieved after one round of encryption. Afterward, figure 13 is generated after 15 rounds and this coded image is highly degraded. Figure 14 illustrates a histogram of the plain image and figure 15 shows the histogram that is produced after one round of encryption. Figure 16 illustrates the more uniform and highly different histogram form the histogram of plain image.

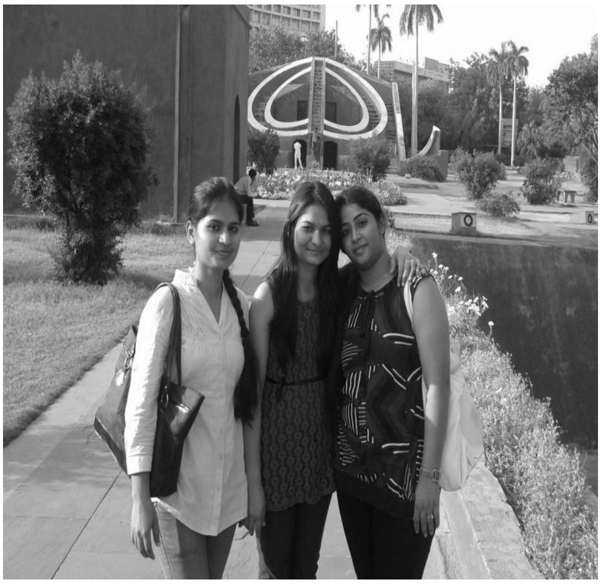

Fig 11: Plain image

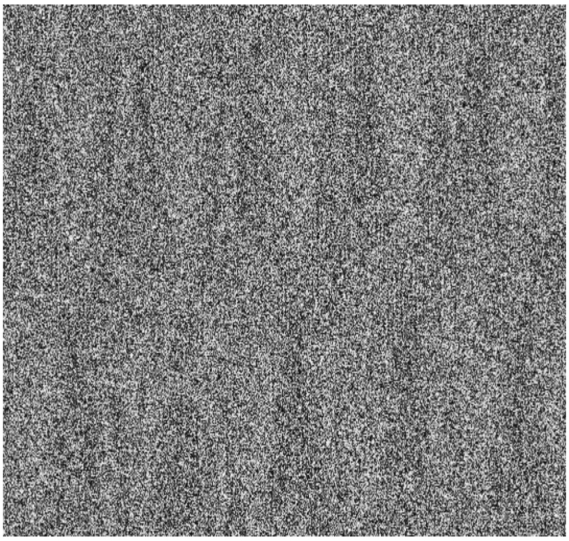

Fig 12: cipher image at round 1

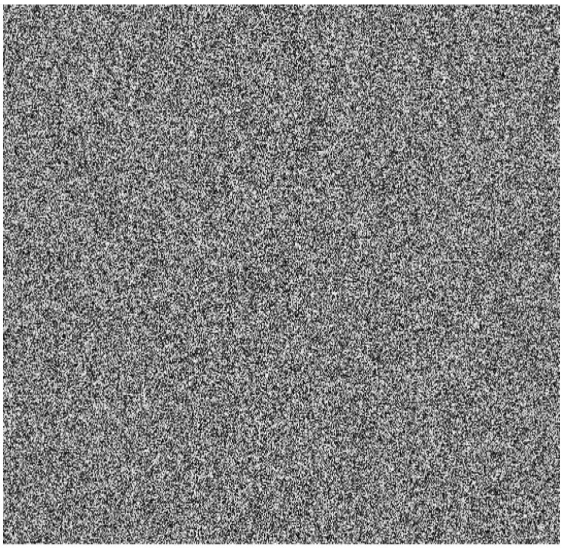

Fig 13: Cipher image at round 15

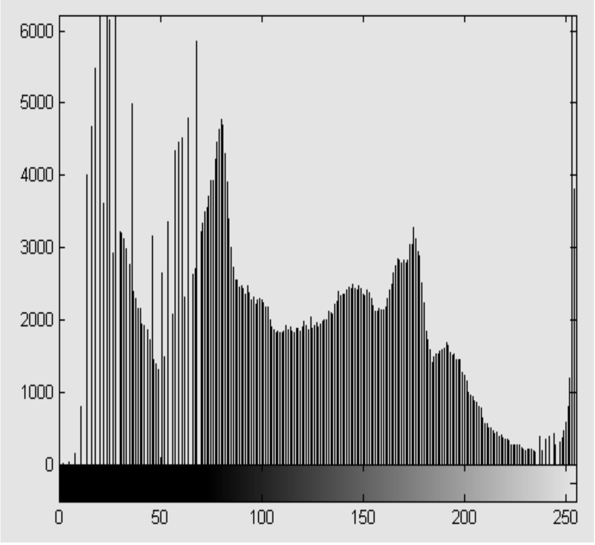

Fig 14: Histogram of plain image

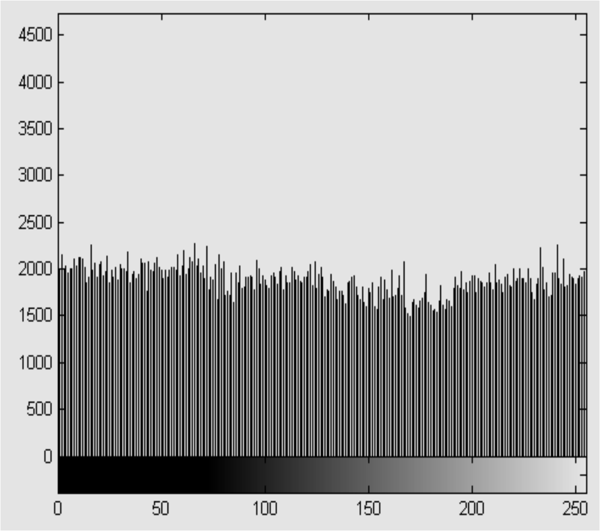

Fig 15: Histogram of encrypted image after one round

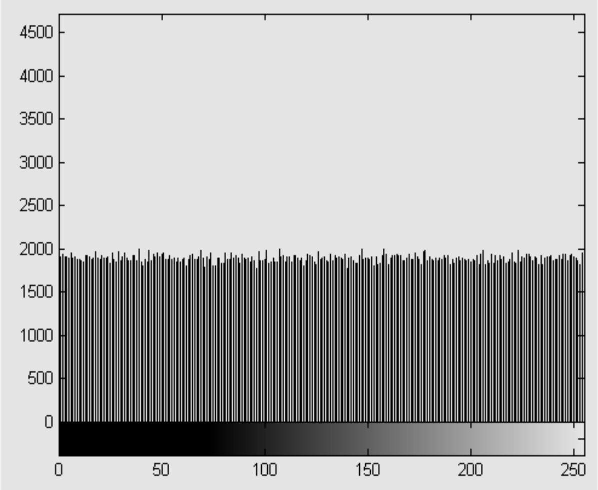

Fig 16: Histogram of encrypted image after 15 rounds

5. CONCLUSION

This paper illustrates that only scrambling process is not sufficient to offer trustable security. There should be a substitution process with the scrambling procedure to increase complexity in histogram analysis. The proposed algorithm applies the both scrambling and substitution process. Consequently, the suggested method provides a more uniform histogram that is different from the histogram of plain image. This uniform histogram creates difficulty in the histogram analysis. This technique does not suffer from the problem that is encountered in algorithm based on one-dimensional scrambling. Thus, imparted technique is more suitable than algorithm based on only one-dimensional scrambling.

6. ACKNOWLEDGEMENTS

Author is thankful to his guides Mr. Akshat Agrawal and Mr. Ankit Garg who give him an opportunity to carry out this work. Author is also thankful to NPTEL which provides effective E-learning through online web and video courses in Engineering and Science.

7. REFERENCES

[1] Yashpalsingh Rajput, A.K. Gulve, “An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher”, International Journal of Computer Applications, volume 83 – no 13, December 2013, pages: 4-8.

[2] Mohammed Abbas Fadhil Al-Husainy, “A Novel Encryption Method for Image Security”, International Journal of Security and Its Applications, vol.6, no.1, January 2012, pages: 1-8.

[3] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar “Image Encryption Using Affine Transform and XOR Operation” 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages : 309-312.

[4] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," in Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002, pp 9-11.

[5] Changgui, B. K Bharat, "An efficient MPEG video encryption algorithm," Proceedings of the symposium on reliable distributed systems, 1998, pp. 381 -386.

[6] Mohit Kumar, Akshat Aggarwal and Ankit Garg, “A Review on Various Digital Image Encryption Techniques and Security Criteria”, International Journal of Computer Applications, Volume-96, no-13, 17 June, 2014, pages:19-26.

[7] Qiudong Sun, Ping Guan, Yongping Qiu, Yunfeng Xue “A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling” 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012, page: 1669-1672.