# Improving Quality of Image in Permutation-Only Image Encryption Schemes

**Aparna N[1] Mrs Kavyashree[2]**
[1]M.Tech. Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]RGIT Bangalore, India

*Abstract*— Permutation is a commonly used primitive in multimedia (image/video) encryption schemes, and many permutation-only algorithms have been proposed in recent years for protection of multimedia data. In permutation only image ciphers, the entries of the image matrix are scrambled using a permutation mapping matrix which is built by a pseudo-random number generator (PRNG). The literature on the cryptanalysis of image ciphers indicates that permutation-only image ciphers are insecure against ciphertext-only attacks and/or known/chosen plaintext attacks. In our proposed work we intend to develop the cipher data by considering two encryption algorithm concerning Arnold Cap Map (ACM) and Chaotic sequential data. In this work we intend to improve the PSNR value of the image.

***Key words:*** Permutation-Only, Ciphertext, Arnold Cap Map, Chaotic Sequential Data, PSNR

## I. Introduction

The recent advancements in the field of Digital multimedia have created a demand with respect to security of the data. Applications such as Pay-Tv, remote video conferencing, and medical imaging demand a secure data which leads to the development of encryption algorithms. Many encryption algorithms has been proposed and developed over the last four decades leading to creating standards pertaining to encryption. Some of the noted and accepted standards over the world include Data Encryption Standard (DES) initially created by IBM on public request, another such standard pertaining to encryption is the Advanced Encryption Standard (AES).

The digital images have a grid like structure which basically involves two operations while performing encryption. They are

- Position permutations: This operation is the most commonly used operation in image encryption. The permutations applicable to both spacial and frequency domains. Its main advantage lies in its easy implementations. permutation dissipates the statistical structure of the plaintext into long range statistics and it is suitable for fast processing requirements of massive digital multimedia data\
- Value Transformation: This operation performs transformation on the image pixel values. Some times in order to obtain a high secured data, the position permutation and a simple value transformation such as XOR operation are performed. Such type of operations involving both the methods could be called as combinational operation.

Parameters relating to image encryption include tunability which is defined as the dynamic definition of the encryption parameters and the encrypted part according to various requirements and applications. Static definition of encrypted part and encrypted parameters helps in scalability for schemes usage. Cryptographic security which defines to know the security of encryption scheme against the plaintext attacks and brute force; and the security is measured as high, medium or low. Speed which defines the faster time for encryption and decryption processing of algorithms. Compression which helps in maintaining the bandwidth of the image while transmission and also helps during the decryption and Visual degradation: This helps in the measurement of the image data perceptual distortion according to with plain image.

The following sections in this paper are as follows. The first section gives a brief introduction concerning the significance of the area of interest and the general problems associated with it. The second section gives a brief introduction regarding the prerequisites necessary for better understanding of the subject. A review of literature and related works is given in section 3. The proposed system and implementation concerning the architecture and work flow of the project is given in section 4 and 5 respectively. The obtained results are given in section 6 and finally the conclusion of the overall work along with references is given.

## II. Literature review

In a view of procuring high efficiency and perfect effect for encryption and decryption of digital images and also considering the high security of the encrypting algorithm, a discrete chaotic encrypting algorithm of digital images had been studied by Z. Dinghui [1], In order to effectively realize digital image encryption and decryption, two one-dimensional discrete Chebyshev chaotic sequences were used for row and column scrambling of the pixels of original and encrypted digital images. Experiment results showed that the encrypting algorithm was reasonably feasible and effective, and could ensure encrypted images sufficient security in their storage and transmitting processes.

In view of addressing the compression issues with respect to encrypted image J. Zhou et al. [2] designed an efficient Encryption Then Compression (ETC) system which considered both lossy and lossless compression. The proposed image encryption scheme operated in the prediction error domain was shown to be able to provide a reasonably high level of security. An arithmetic coding-based approach could be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images was only slightly worse, in terms of compression efficiency, than the state-of-the-art lossless/lossy image coders, which take original, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency.

S. Rahman et al [3]. proposed a chaos cryptographic based scrambling approach which could be applied on selected region of interest (ROI) in video camera footage which contains privacy sensitive data. The result obtained was a good balance between hiding privacy sensitive material and effective supporting of surveillance tasks.

T. Uehara et al. [4] shows that in block-based DCT, it is possible to recover dc coefficients from ac coefficients with reasonable image quality and show the insecurity of image encryption methods which rely on the encryption of dc values using a crypto algorithm. The method combines dc recovery from ac coefficients and the fact that ac coefficients could be recovered using a chosen cipher-text attack.

L. Zhao et al. [5] proposes an improved image scrambling encryption scheme which is based on the idea of 'self-correlation' method which resists the chosen-plaintext attack/known-plaintext attack. The corresponding simulations and analyses illustrate that the improved encryption method has good cryptographic properties, and could overcome the weakness of the original image encryption scheme proposed in their work.

In view of the weakness of pure position permutation algorithm, X. Zhao et al. [6] put forward an effective decryption algorithm for all pure-position permutation algorithms. By using probability theory and algebraic principles, the decryption probability of pure-position permutation algorithms was verified theoretically; and then, by defining the operation system of fuzzy ergodic matrices, they improved the specific decryption algorithm.

To address the correlation issues, Matias and Shamir [7] proposed a permutation-only scheme which scanned pixels in a highly irregular scanning pattern using a pseudo-random space filling curve.

Bertilsson et al. [8] then showed that Matias and Shamir's permutation method is vulnerable to a ciphertextonly attack. They showed that the pixel data could be reordered according to a space-filling curve, and hence, the plain-image could be partially recovered by exploiting the correlation between subsequent frames.

Kuhn [9] presented a more advanced approach to break the video signal scramblers commercially employed within pay-TV conditional access encryption systems [10], such as EuroCrypt, VideoCrypt and Nagravision, using ciphertext-only attacks. Kuhn showed that the long portion of the permuted lines/segments makes the correlation attacks on the scrambling algorithm feasible by comparing and matching lines/segment portions.

Li et al. [11] then extended Kuhn's work by analyzing the permutation domain of particular image encryption schemes with longer permutation domains, such as the row-column permutation-only encryption scheme of [1].

## III. IMPLEMENTATION

The objective of the proposed system is to perform diffusion based encryption/ decryption with respect to bit level encryption/ decryption and chaotic based encryption/ decryption for pixel relocation. The obtained decrypted image will be sent to the noise removal process where a spatial based filtering will be applied for the purpose of noise correction. The PSNR value is considered as a standard of measure for the quality of the noise corrected image and the correlation coefficient is considered as a measure for the performance of the encryption/ decryption methods. the proposed system architecture is shown in fig X. which involves four modules, they are encryption, key generation, decryption and noise removal.

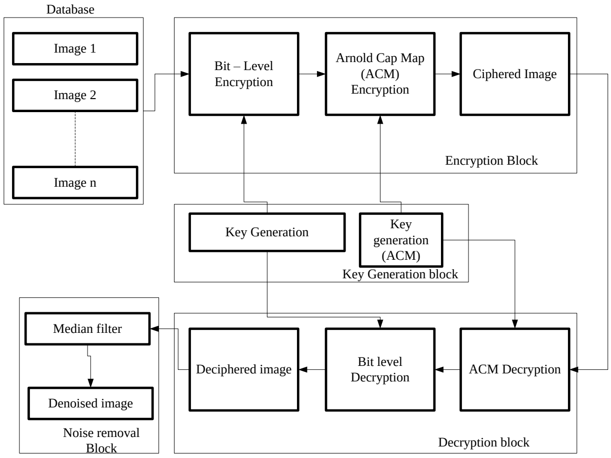

Fig. 1: Proposed Methodology

Initially an input image (plain image) is resized to have an equal dimension of square matrix. A bit level encryption is performed where the a key is generated having the same number of rows as the number of total bytes and the 1 column. Each bit in the plain image is XORed with the value of the corresponding position of the key. The resulting encrypted image is then sent to the chaotic based mapping encryption which in this case the Arnold Cap map based scrambling method is used to scramble. a number of iteration for the ACM is specified by the user. the key with respect to ACM is generated by first entering a value which in turn produces a random number, the value of this random number is considered as the number of iterations for the ACM encryption method to be performed. The resulting image is the ciphered image which is expected to have a high correlation coefficient with respect to image pixels.

The decryption of the image is performed by first considering the ciphered image obtained by the ACM method. The user will be prompted for a key, this is the same key which was set during the ACM encryption process. Upon entering the respective key the iteration value is retrieved which will perform the same number of iteration as was performed during the ACM encryption process. The decrypted image from ACM method is then sent to the bit level diffusion based decryption method where the user is prompted for the second key which was created during the encryption process of the bit level encryption method. Upon receiving the key the pixel position of the decrypted image is XORed with the corresponding pixel position of the key. The resulting image is the final decrypted image. The final decrypted image is sent to the noise removal process where a spatial based median filter is applied which in turn improves the quality of the image with respect to its psnr value.

## IV. SIMULATION RESULTS

This chapter deals with the simulated results obtained from the implementation of the project with respect to image encryption/ decryption process along with noise removal. The following sections are mentioned as follows. The first section deals with the brief mentioning of the structure and attributes of the database with respect to images. The second section performs an analysis of the outcome of the simulation.

The database considered for implementation in this project consists of five images of type unsigned integer (8 bits) with the following attributes mentioned in table 1.

| Sl. No | Input | Image format | Image size | Bytes | Class | Min. value | Max. value |
|---|---|---|---|---|---|---|---|
| 1 | Input1 | .jpg | 256 X 256 | 65536 | Uint(8 bits) | 0 | 255 |
| 2 | Input2 | .png | 256 X 256 | 65536 | Uint(8 bits) | 3 | 245 |
| 3 | Input3 | .jpg | 560 X560 | 313600 | Uint(8 bits) | 0 | 255 |
| 4 | Input4 | .jpg | 600 X 600 | 360000 | Uint(8 bits) | 5 | 255 |
| 5 | Input5 | .jpg | 750 X 750 | 562500 | Uint(8 bits) | Exceeds Lt. | Exceeds Lt. |

Table 1: Database for the implementation of the project

### A. *Result Analysis*

The observations made with respect to proposed system is shown in table.2

### B. *Peak-Signal-to-Noise Ratio (PSNR):*

The Peak Signal to Noise Ratio (PSNR) is used as a quality measurement between the original and a reconstructed image. PSNR usually expressed in terms of logarithmic decibel value. The PSNR is calculated as shown in eq.1

$$PSNR = 10 \log_{10}\left(\frac{max^2}{MSE}\right) \qquad \text{.....(1)}$$

Where, max→ maximum fluctuation in an input image

MSE→ mean square estimation

### C. *Correlation Coefficient:*

Correlation coefficient is computed to find the measure of relativity between two samples of interest. The mathematical representation is as shown in eq.2.

$$r = \frac{n(\sum_i xy) - (\sum_i x)(\sum_i y)}{\sqrt{[n\sum_i x^2 - (\sum_i x)^2][n\sum_i y^2 - (\sum_i y)^2]}} \qquad \text{......(2)}$$

Where, r→ correlation coefficient
n→ total number of elements
i→ Number of elements in x and y (individually)
x→ first sample
y→ second sample

| sl.no | Input image | PSNR (Decrypted image) | PSNR (Noise corrected image) | Improved PSNR (%) | correlation coefficient |
|---|---|---|---|---|---|
| 1 | Input1 | 17.6001 | 24.4917 | 39.1571 | 0.0375 |
| 2 | Input2 | 17.7218 | 25.6168 | 44.5503 | -0.0115 |
| 3 | Input3 | 18.5405 | 27.3936 | 47.74 | -0.0115 |
| 4 | Input4 | 17.8421 | 28.9892 | 62.4758 | 0.0108 |
| 5 | Input5 | 15.6754 | 26.8863 | 71.5189 | 0.0082 |

Table 2: Observations with respect to the proposed system

## V. Conclusion

The diffusion based encryption and decryption methods are successfully performed by applying value based transformation and position based transformation respectively. The bit level encryption/ decryption is used for value based transformation and the chaotic based encryption/ decryption is used for position based transformation by using the ACM method. Individual keys are generated for the above encryption operations. It is observed that the correlation coefficient is significantly reduced with respect to image pixels when compared to ACM only encryption method. A spacial based filtering approach is performed for the purpose of improving the image quality with respect to its psnr values. It is also observed that the psnr value of noise corrected image increases as the dimension of the respective image increases.

## References

[1] Z. Dinghui, G. Qiujie, P. Yonghua, and Z. Xinghua, “Discrete chaotic encryption and decryption of digital images,” in Proc. Int. Conf. Comput. Sci. Soft. Eng., Wuhan, China, pp. 849–852, 2008.

[2] J. Zhou, X. Liu, O.C. Au, and Y.Y. Tang, “Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation,” IEEE Trans. Inf. Foren. Sec., vol. 9, no. 1, pp. 39–50, 2014.

[3] Sk. Md. Mizanur Rahman, M.A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, “Chaos-cryptography based privacy preservation technique for video surveillance,” Multim. Sys., vol. 18, no. 2, pp. 145–155, 2012.

[4] T. Uehara and R. Safavi-Naini, “Chosen DCT coefficients attack on MPEG encryption schemes,” in Proc. IEEE Pacific Rim Conf. Multim. (IEEE-PCM’2000), pp. 316–319, 2000.

[5] L. Zhao, A. Adhikari, D. Xiao, and K. Sakurai, “On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption,” Comm. Nonlinear Sci. Numer. Simulat., vol. 17, no. 8, pp. 3303–3327, 2012.

[6] X.-Y. Zhao, G. Chen, D. Zhang, X.-H. Wang, and G.-C. Dong, “Decryption of pure-position permutation algorithms,” J. Zhejiang Univ. Sci., vol. 5, no. 7, pp. 803–809, 2004.

[7] Y. Matias and A. Shamir, “A video scrambling technique based on space filling curves,” in Proc. Advances in Cryptology–Crypto’87, Lecture Notes in Computer Science, vol. 293, C. Pomerance, Ed., Springer, pp. 398–417, 1987.

[8] M. Bertilsson, E.F. Brickell, and I. Ingemarson, “Cryptanalysis of video encryption based on space-filling curves,” in Proc. Advances in Cryptology–EuroCrypt’88, Lecture Notes in Computer Science, vol. 434, Springer, Berlin, pp. 403–411, 1989.

[9] M. Kuhn, “Analysis for the Nagravision video scrambling method,” 1998, online document, available at: http://www.cl.cam.ac.uk/ mgk25/ nagra.pdf.

[10] J. McCormac, European Scrambling Systems 5: Circuits, Tactics And Techniques – The Black Book, Waterford University Press, 1996.

[11] W. Li, Y. Yan, and N. Yu, “Breaking row-column shuffle based image cipher,” in Proc. 20th ACM international conference on Multimedia (MM’12), New York, NY, USA, pp. 1097–1100, 2012.