

1133-49-37

**Debasis Giri\*** (debasis\_giri@hotmail.com), Dean, College of Computer Science, Haldia Institute of Technology, HALDIA, WestBengal , India. *An Optimal method for Image Encryption based on Random Vectors.*

We will discuss an image encryption method based on changing the pixel positions as well as pixel values to confuse the relationship between the cipher image and the plain-image using four random shared secret vectors and two secret numbers. In the proposed method, four random vectors are generated according to the size of the image which acts as a key for this encryption algorithm. One of the random vectors is used to shuffle the first row and then the random vector is modified using two random integers which are relatively prime with the size of the image. Same process is repeated for the other rows of the image. We then shuffle the pixels of columns as the method of rows shuffling using another random vector. The diffusion process is carried out by other two random vectors, one for row and the other for column. The pixel values are changed using simple exclusive-or operation and shifting operation.

From the results, it is observed that the proposed technique significantly reduces the correlation among the pixels by shuffling the image matrix using the random vectors. . The use of four random vectors increases the key space which provides better security against Brute Force Attack. (Received June 16, 2017)