Image Encryption and Compression using Scan Patterns

Shalin J Patel[1]
[1]Department of Electronics & Communication Engineering
[1]Kalol Institute of Technology and Research Center, Kalol

Abstract— today image compression and encryption has been a great area of interest since images are being used as one of the most valable information source in many areas like medical, information technology, rocket science application and many more. There are mainly types of image are three namely binary, grayscale and color image. Binary image has only two intensity levels black and white, on other hand grayscale images have 256 intensity levels and at last color images have various color map each of which have 256 intensity levels. Our scope is limited up to only grayscal images. The methodology here we used for image compression and encryption is by using scan pattern which is an algorithm which is capable of doing both and encryption as well as compression of an image simultaneously. It is a method applied on binary images. The methodology is applied on grayscale sample images, by dividing the grayscale image into its corresponding bit planes. Aim of the algorithm here is to find a scan path which is capable to compress an image using least bits required. To compression an image we are using run-length coding. The encryption is done also done by using a scan path which is kept secretly and we can use it to generate key and our key length is 232 bits we is much more capable to encrypt the image and is there is any variation in key it will result in failure to get original image which shows the robustness of the algorithm.

Key words: Encryption, Compression, Scan, Histogram, Run Length Encoding, Correlation, Key

I. INTRODUCTION

To secure the image is an important issue in communication amd solution is encryption. Image encryption has a wide range of applications in inter-net communication, multimedia systems, medical imaging, telemedicine, and military communication. Number ofl image encryption methods are exists like SCAN, tree structure, chaos-based methods, and some miscellaneous methods. Every method has its own strengths in terms of security level, speed, and stream size metrics.

The proposed image encryption method is based on rearrangement of the pixels of the image. The rearrangement is done by scan patterns that generated by the SCAN methodology[8]. The scanning path of the image is a random code form, and by specifying the pixels sequence along the scanning path. Note that scanning path of an image is simply an order in which each pixel of the image is accessed exactly once. Such an encryption also involves the specification of set secret scanning paths. Therefore, the encryption needs a methodology to specify and generate a larger number of wide varieties of scanning paths effectively.

The scanning is the process which transforms the 2-dimensional image into 1-dimensional vector. Various image scanning algorithms focus on the nearby pixel similarity in the image. They are designed to exploit this characteristic to improve the autocorrelation in the resulting 1-dimensional image representation. Image scanning using SFCs is a typical example of such algorithm [2].

II. GENERIC SFCS

An SFC defines a continuous scan that traverses through image pixels exactly once. The resulting sequence of pixels is then processed as required by the corresponding application. To obtain the image after processing, the (possibly modified) pixel-sequence is placed back in a frame along the same SFC. In compression, it is important that the intra-pixels correlation in the image is translated to an appropriate autocorrelation within the pixel-sequence [3]. It is worth mention that SFCs are explored in order replace the conventional line-scan by other forms of more appropriate scans. The researches done mejoritily converge to fractal curves. Additionally, the scan-line is a standard scanning method, which traverses a frame line by line. It is well known. Intuitively, the recursive nature of the SFC requires it to traverse neighboring pixels before moving to more distant ones, resulting in better exploitation of the two-dimensional locality.

These SFCs tend to minimize the differences between the Intra pixel distances in the image (distances in 2D image space) and ones in the generated pixel sequence (1D representation).

III. BASIC INTRODUCTION TO SCAN

A scanning of a 2-D array as defined by S.S.Maniccam and N.G.Bourbakis is nothing but an order in which each and every element of that array is accessed only and exactly once. In this report the words scanning, scan patterns, scan paths are used interchangeably. So as an element is processed only once in an array, an (NxN) array will have (NxN)! scanning. Which means an 4x4 2-D array will have (16)! or 20922789888000 scannings. Here in figure two different scanning's has been shown on a 4x4 array among which one is widely used raster scanning [6].

The Scan is a formal language which is -based on two dimensional spatial accessing methodologies which can represent and generate a large number of wide varieties of scanning paths. The SCAN is a family has languages such as Generalized, Simple, and Extended Scan each of which can represent as well as generate a set of scanning paths. Each language of Scan is defined by a set of basic scan patterns, set of rules to recursively compose simple scan patterns and set of partition patterns to obtain complex scan patterns and transformations with scanning or partitioning. A scanning of a two dimensional array P = {p(i, j): $1 \le i \le x$, $1 \le j \le y$} is a bijective function from P to the set{1,2,…,pq-1,pq} [2]. In other world, a scanning of a two dimensional array is an order in which each element of the array is accessed exactly once the terms scanning, scanning paths, scan pattern, and scan words are used interchangeably. If there are array of m x n then it has (m x n)! scanning.

All rights reserved by www.ijsrd.com

IV. ENCRYPTION & DECRYPTION

A. Encryption:

To encrypt image divide the gray scale image into 8-bit planes. Take Nth plane and divide the plane into four segments according to path decided in key. Apply relative partition pattern. Apply relative scan pattern to each partition. Repeat it for all the planes. Recompose the image. Divide the image into four segments and apply scan pattern, resultant image is an encrypted image.

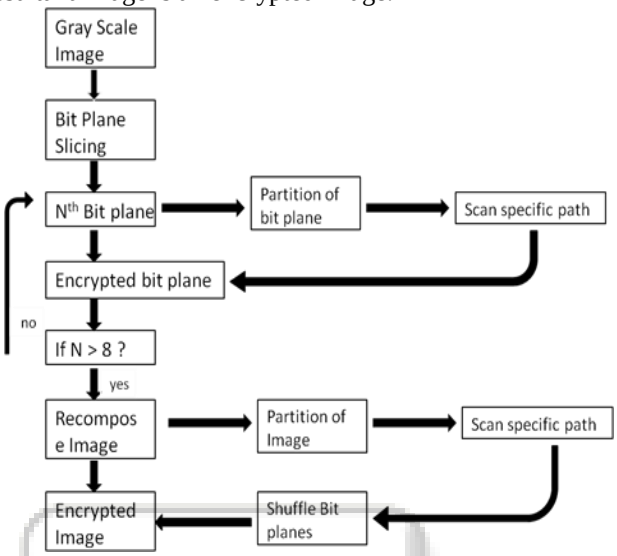

Fig. 1: Encryption Diagram

B. Decryption:

To decrypt the image divides the image into four segments and apply scan pattern. Decompose the image into 8 bit Planes. Take ith plane and divide the plane into four segments according to path decided in key. Apply relative partition pattern. Apply relative scan pattern to each partition. Repeat it for all the planes. Recompose the (Decrypted) image.

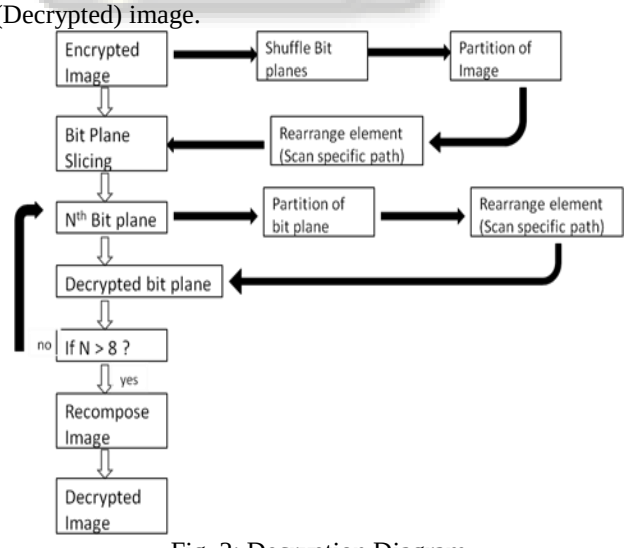

Fig. 2: Decryption Diagram

C. Types of Patterns:

Here we are using 8 different scan patterns to encrypt the image. Each scan patterns has given their own number so that it is helpful in key generation. Suppose if we use second pattern as the encryption path then in encryption we write 010 in place that pattern.

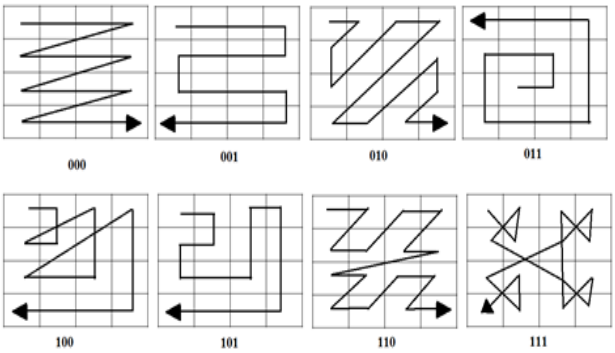

Fig. 3: Types of patterns

These blocks are used to divide the image into sub images or blocks. We have used three block partition 01 as B type partition 10 as X type partition and 11 as Z type partition block partition. This can also be used in encryption key.

D. Shuffeling Schemes:

We have introduced these 8 different shuffling schemes to shuffle the bit planes.suppose if we have use 001 as shuffling scheme the first bit plane is replaced by forth ,third with first like this all the bit planes will get shuffled.

000-34215678	001-41378652	010-23416785	011 - 13248675
100-32415876	101-21437586	110-41326758	111 - 14328576

E. Key Generation:

We are using 0000 as the start bit. Then we divide the image into 8 different planes. Now first plane will come so plane no is 000.now we divide image into 4 blocks. That four blocks are shuffled by partition type 01 to 11.we apply scan pattern to each and every block and every block will use different can pattern. Suppose for first block pattern type use is forth than key will be 00 for first block and 100 for forth block. By applying this to all the planes we shuffle the bit planes by any scheme like 011.After that we apply another same methodology for double encryption and that data is arranged as 1-d data. After applying RLE we will get compressed image.

V. RESULTS

Fig. 4: Lena.jpg

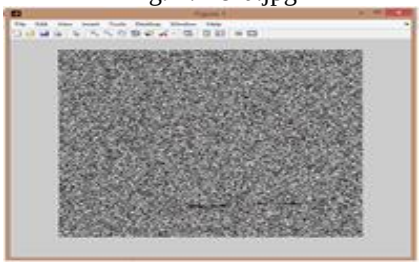

Fig. 5: Encrypted Image of Lena.jpg

All rights reserved by *www.ijsrd.com*

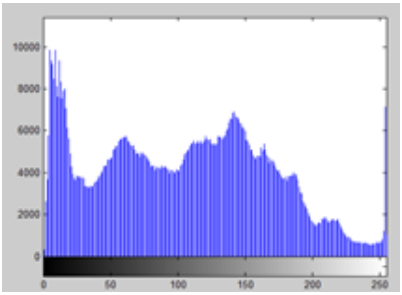

Fig. 6: Histogram of Lena.jpg

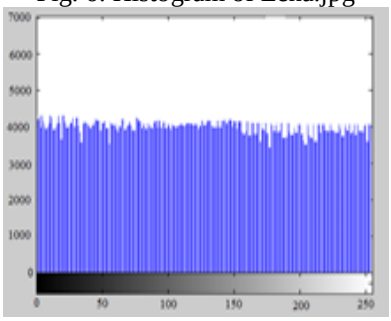

Fig. 7: Histogram of En-crypted Image of Lena.jpg

	Original Image	**Cipher Image**
Correlation	0.6987	0.0098
Entropy	7.2149	7.8652
NPCR (%)	-	99.9345
UACI (%)	-	33.9221

Table 2: Comparison Between Original And Encrypted Image

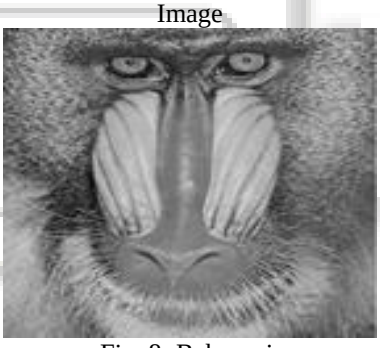

Fig. 8: Baboon.jpg

Fig. 9: Encrypted image for Baboon.jpg

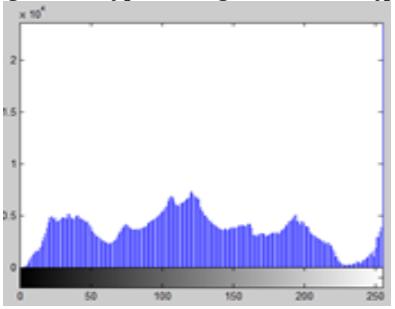

Fig. 10: Histogram of Baboon.jpg

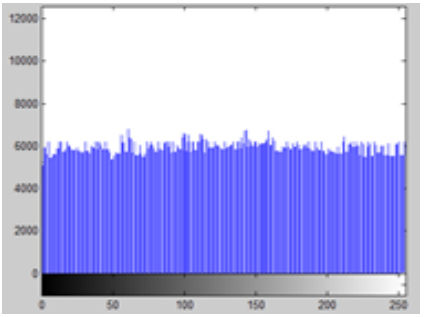

Fig. 11: Histogram of En-crypted image for Ba-boon.jpg

	Baboon.jpg	**Encrypted Image**
Correlation	0.6987	0.0098
Entropy	7.2149	7.8652
NPCR (%)	-	99.9345
UACI (%)	-	33.9221

Table 3: Comparison between Original and Encrypted Image

VI. CONCLUSIONS

In this paper, we have proposed a very new improved approach for image security using a combination of image compression and encryption techniques is proposed. This approach uses Scrambling of image pixels to reduce correlation. Inter pixel redundancy can be reduced by using this scan methodology. According to scan pattern used we will get the encryption key and image as 1-D data. The results we get after experiment show that the proposed image encryption system has a very large key space 232 bits and also the cipher image has entropy information close to the ideal value 8 and low correlation coefficient .The ideal value of correlation coefficient is 0 and we are very near to it. Thus the analysis proves the robustness, security, effectiveness of the proposed image encryp-tion algorithm.

As a future work its required to find the better way to find the scan path by which we get highest compression ratio.It also in-cludes the modification of the compression method so that it can be applied on the intensity level for grayscale image directly, doing this compression time can be minimized and the correlations between the pixels can be exploiting better.

We can also do the encryption on color images by separating the three color planes and then apply the same algorithm. The speed of the algorithm is quite slow so have to find way speed.

REFERENCES

[1] Lossless image compression and encryption using SCAN, S.S. Maniccam, N.G. Bourbakis Pattern Recognition, Elsevier, Volume 34, Issue 6, June 2001, Pages 1229–1245

[2] SCAN Based Lossless Image Compression and Encryption S. S. Maniccam, N. G. Bourbakis, Binghamton University, Dept. EE, Image-Video-Machine Vision Lab, Binghamton NY 13902, U.S.A. Technical University of Crete, Dept. ECE, Chania 731 00, Crete, Greece

[3] Image Encryption and Decryption Using SCAN Methodology Chao-Shen Chen ; Rong- Jian Chen Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International

All rights reserved by *www.ijsrd.com*

Conference on Digital Object Identifier: 10.1109/PDCAT.2006.71 Publication Year: 2006 , Page(s): 61 – 6

[4] An Introduction to Image Compression, Wei-Yi Wei, Graduate Institute of Communication Engineering National Taiwan University, Taipei, Taiwan, ROC

[5] N. Bourbakis, C. Alexopoulos, Picture data compression using SCAN patterns, SPIE Conference on Electronic Imaging, February 1993.

[6] G. Drost, SCAN based lossless image compression application specific integrated circuit, Masters Thesis, SUNY Binghamton, 1998.

[7] The comparisons between public key and symmetric key cryptography in protecting storage systems Lanxiang Chen ; Shuming Zhou Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 4 Digital Object Identifier: 10.1109/ICCASM.2010.5620632 Publication Year: 2010 , Page(s): V4-494 - V4-502.

[8] C. S. Chen and R. J. Chen, ―Image Encryption and Decryption Using SCAN Methodology‖, Seventh International Conference on Parallel and Distributed 33 Computing, Applications and Technologies, PDCAT, IEEE, Taipei,

[9] Rajan Gupta, Ankur Aggarwal, and Saibal K. Pal. ―Design and Analysis of New Shuffle Encryption Schemes for Multime-dia.‖Defence Science Journal, Vol. 62, No. 3, May 2012, pp. 159-166, DOI: 10.14429/dsj.62.1008

[10] Kamlesh Gupta, Sanjay Silakari. ―New Approach for Fast Color Image Encryption Using Chaotic Map.‖Journal of Infor-mation Security, 2011, 2, 139-150

[11] Xiaoyi Zhou*1,2, Jixin Ma. ―Ergodic Matrix and Hybrid-key Based Image Cryptosystem‖.I.J. Image, Graphics and Signal Processing, 2011, 4, 1-9 Published Online June 2011 in MECS

[12] KamelFaraoun. ―Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption‖.The International Arab Journal of Information Technology, Vol. 7, No. 3, July 2010

[13] Jilali MIKRAM, Fouad ZINOUN, Mouad HAMRI. ―An Encryption Algorithm Based on the Decimal Expansion of Irra-tionals.‖ Applied Mathematical Sciences, Vol. 6, 2012, no. 70, 3475 – 3494

All rights reserved by *www.ijsrd.com*