Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(4): 23-30

Research Article ISSN: 2394 - 658X

Combination of DNA Sequence in Scan Patterns and Dyadic Permutation in Securing the Image Contents

Nandish M and Kailash Rudra

Department of Computer Science and Engineering,
PES Institute of Technology and Management, Shimoga, Karnataka State, India
nandish.m@pestrust.edu.in

ABSTRACT

With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is true that a large part of the information is either confidential or private. As a result, different techniques have been used to provide the security. The security of digital images has attracted more attention and many different image encryption methods have been proposed to enhance the security of the images. Digital data security is achieved by methods of cryptography, which deals with encryption of data. The common method of protecting the digital documents is to scramble the content so that the true message of the documents is unknown. The proposed method combines the concept of scan patterns and dyadic permutation. Scan patterns shuffles the pixels of the image and dissipate the high correlation among pixels. Dyadic permutation process performs repositioning of the pixels in the image. Carrier images are generated using random sequence based on DNA. Carrier image has been used for encrypting and decrypting images. The system is tested for different types of images of different size. The results obtained are analyzed through histograms and correlation coefficient which shows that the developed system is working satisfactorily.

Key words: Image encryption, SCAN patterns, Dyadic Permutation, Correlation

INTRODUCTION

Now a day's security incidents are getting more importance. As the complexity of the threats and attacks increases, so do the security measures required to protect them also. Network administrators, data centre operators, and other data centre professionals need to comprehend the basics of security in order to safely manage the information. Controlling physical access to machines and network attach points is perhaps more critical than any other aspect of security. Any type of physical access to an internal site creates a major exposure of the site. It is important to be concerned about revealing information that is exchanged between, computers, systems or network elements. When one wishes to avoid data disclosure over a network, encryption techniques must be employed that make the transmitted data unreadable to someone who is not intended receiver. The SCAN based encryption throws light upon scan pattern generation algorithm. The SCAN is a formal language based two dimensional spatial accessing methodologies which can represent and generate a large number of wide variety of scanning paths or space filling curves easily. The main advantage of the SCAN algorithm is its strong encryption rather than its high throughput. Dyadic permutation can be a very useful tool for digital image coding and decoding, digital image quality analysis, digital pattern reconstruction and quality control of binary objects such as gratings. Dyadic permutation of an image can be interpreted as a special type of permutations of its pixel addresses. Dyadic permutation can be used to encrypt the information contained in the pictures without information loss or damage. DNA cryptography makes encryption more strong and secure and protect from brute force attacks. It also offers high confidential strength and large storage density inherent in it, as compare to the traditional storage devices.

In this paper, image encryption scheme based on scan patterns and dyadic permutation are presented. Rest of the paper is organized as follows. A related literature survey is carried out in Section 2. In Section 3, an overview of SCAN patterns is described. An overview of dyadic's, dyadic group, and dyadic permutation in encryption are presented in Section 4. In Section 5, the proposed method is explained along with an algorithm. Experimental results are discussed in Section 5. Statistical analysis of the results is presented in Section 6. Conclusions are drawn in Section 7.

LITERATURE SURVEY

Maniccam and Bourbakis [1] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language based two dimensional spatial accessing methodologies which can efficiently specify and generate a wide range of scanning paths or space filling curves. In [2], Castaneda et al discussed an encryption method based on dyadic permutation. Dyadic displacements of an image can be interpreted as a special type of permutations of its pixel addresses. Dyadic displacements can be a very useful tool for digital image coding and decoding, digital image quality analysis, digital pattern reconstruction and quality control of binary objects such as gratings. Dyadic displacements can be used to encrypt the information contained in the pictures without information loss or damage. The information recovery can be performed successfully by using dyadic correlations.

Zhang et al [3] described DNA cryptography-based image encryption. DNA sequences are used as the secret keys. The permutation process is implemented by using Hao's fractal sequence representation and the diffusion process is used to alter the gray values. An image encryption approach is based upon DNA fractal. This approach is not the one based on the real DNA cryptography, but uses the natural DNA sequences as the secret keys. A simple visualization method based on counting and coase-graining is proposed in [4]. When applying the method to all known complete genomes, fractal-like patterns emerge. The fractal dimensions are basic and important quantities to characterize the fractal. Hao et al proposed a DNA fractal sequence representation approach, in which, given a complete genome of length *N*, i.e., a linear or circular DNA sequence made of *N* letters from the alphabet A,C,G and T . Pakshwar et al [5] have presented image encryption using random scrambling and exclusive-or operation (XOR). The pixel of image is highly correlated to their neighboring pixels. Due to this strong correlation any pixel can be practically predicted from a value of its neighbors. Scrambling technique shuffles the pixels of image and scrambled image is called transformed image. The transformed image is then divided into 2 x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total size of key in the algorithm is 32 bit long which proves to be strong enough. The encryption algorithm has been tested on some Gray Scale images and showed good results. In [6], Panduranga et al proposed a hybrid technique for image encryption which employs the concept of carrier image and SCAN patterns generated by SCAN methodology. The carrier image is created with the help of alphanumeric keyword. Each alphanumeric key will be having a unique 8 bit value generated by 4 out of 8-code. The newly generated carrier image is added with original image to obtain encrypted image

From the literature survey it is noticed that many security problems can be solved using SCAN patterns, dyadic permutation and DNA encryption. Various SCAN patterns are used in SCAN algorithm. The selection of secret key in dyadic permutation plays an important role in encrypting the information. In this paper, random selection of secret pair of keys in dyadic permutation and seed value in pseudorandom generator used to create the carrier image is proposed to enhance the image security.

SCAN PATTERNS

The SCAN is a formal language based two dimensional spatial accessing methodologies which can represent and generate a large number of wide variety of scanning paths or space filling curves easily. SCAN is a class of formal languages, which can be applied to compression, encryption, data hiding, or combinations of compression and encryption. SCAN language is an image preprocessing language, devoted to generate a family of 2D scanning. The scanning path of the image is a random code form, and by specifying the pixels sequence along the scanning path. Scanning path of an image is simply an order in which each pixel of the image is accessed exactly once. The 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 [1]. A scanning of a two dimensional array is an order in which each element of the array is accessed exactly once. SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S. Each basic pattern has eight transformations numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are reverses of transformations 0, 2, 4, 6, respectively.

The properties of the SCAN image encryption method, which include pixel rearrangement, confusion, and diffusion. The main advantage of the SCAN algorithm is its strong encryption rather than its high throughput. The SCAN language provides a family of transformations from 2-D to 1-D representations. Each SCAN pattern defines a transposition of the image data into a 1-D representation. Thus, the family of the SCAN patterns could be considered as a transposition cipher. The scan word (or permutation) defines the encryption and decryption key. The scan patterns and transformations are shown in Fig. 1.

In SCAN based encryption, keys are generated using scan alphabets with the transformation. Once the pair of keys are generated, two dimensional strings of length 2^n*2^n where n=0, 1, 2… is converted to one dimensional string by scanning the two dimensional array using keys.

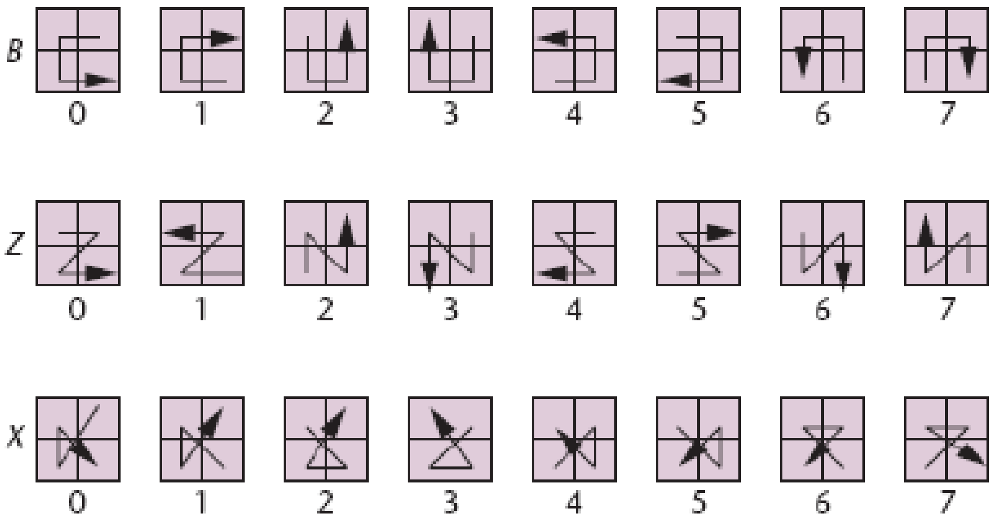


Fig. 1 Scan patterns partition patterns and transformations

DYADIC PERMUTATION

A dyad is a quantity that has magnitude and two associated directions. A dyad is constructed from a pair of vectors (u and v) written side by side as uv, with no operation defined between the vectors. Dyadic displacements can be a very useful tool for digital image coding and decoding, digital image quality analysis, digital pattern reconstruction and quality control of binary objects such as gratings. Dyadic displacements of an image can be interpreted as a special type of permutations of its pixel addresses. Dyadic displacements can be used to encrypt the information contained in the pictures without information loss or damage [2].

A digitized image that captured by a CCD sensor or analyzed by a digital image processing device, can be represented as a 2-D digital function $f\ (n,\ m)$. It can be defined as an array of $N \times M$ pixels. Both the indices n and m denote the addresses of the function values, and $n = 0, 1,..., N - 1$ and $m = 0, 1,...,M - 1$.

Performing the XOR operation with binary digits $j \in [0,N - 1]$ and $k \in [0,M - 1]$, respectively, on the addresses of a 2-D function, i.e. $f(n, m) \rightarrow f(n \oplus j, m \oplus k)$, is called the dyadic displacement of that function. It exhibits the following properties:

i. Closure: The new addresses will have the same number of bits as the original ones.

ii. One-to-one mapping: If a set of data 0, 1,2, 3 is processed by the XOR operation, for example the binary-digit representation of the key is 01, then the result is shown as follows:

$$00 \oplus 01 = 01$$
$$01 \oplus 01 = 00$$
$$10 \oplus 01 = 11$$
$$11 \oplus 01 = 10$$

Both the domain and the region are within the same range [0, 3]. Therefore, if an image is processed by the XOR operation, then the processed image will have the same amount of pixels as the original one.

iii. Reversibility: Each original address can be recovered by the XOR operation of the corresponding encrypted address using the correct key, because $(x \oplus \text{key}) \oplus \text{key} = x$.

iv. Address permutation: The relative position of groups of function values is exchanged by a permutation rule.

THE PROPOSED METHOD

The approach proposed in this section comprises three stages namely SCAN process, dyadic permutation and carrier image generation. The block diagram of the proposed system is shown in Fig. 2.

The proposed method is carried out on standard color image as an input image and secured image transmission is performed by applying encryption. Fig. 4.1 gives the system design to encrypt an input image. The encryption of an image begins with dyadic permutation algorithm. In dyadic permutation, first pair of values is chosen by user in order to perform exclusive or operation on the image pixel address, which is called as dyadic displacements of an image. Dyadic displacements of an image can be interpreted as a special type of permutations of its pixel addresses. The new addresses will have the same number of bits as the former ones. Exclusive-or operation results the intermediate encrypted image which is used for generation of correlated image. Next, correlated image is generated using the dyadic correlated equation. Dyadically shifted image is used an input to SCAN algorithm.

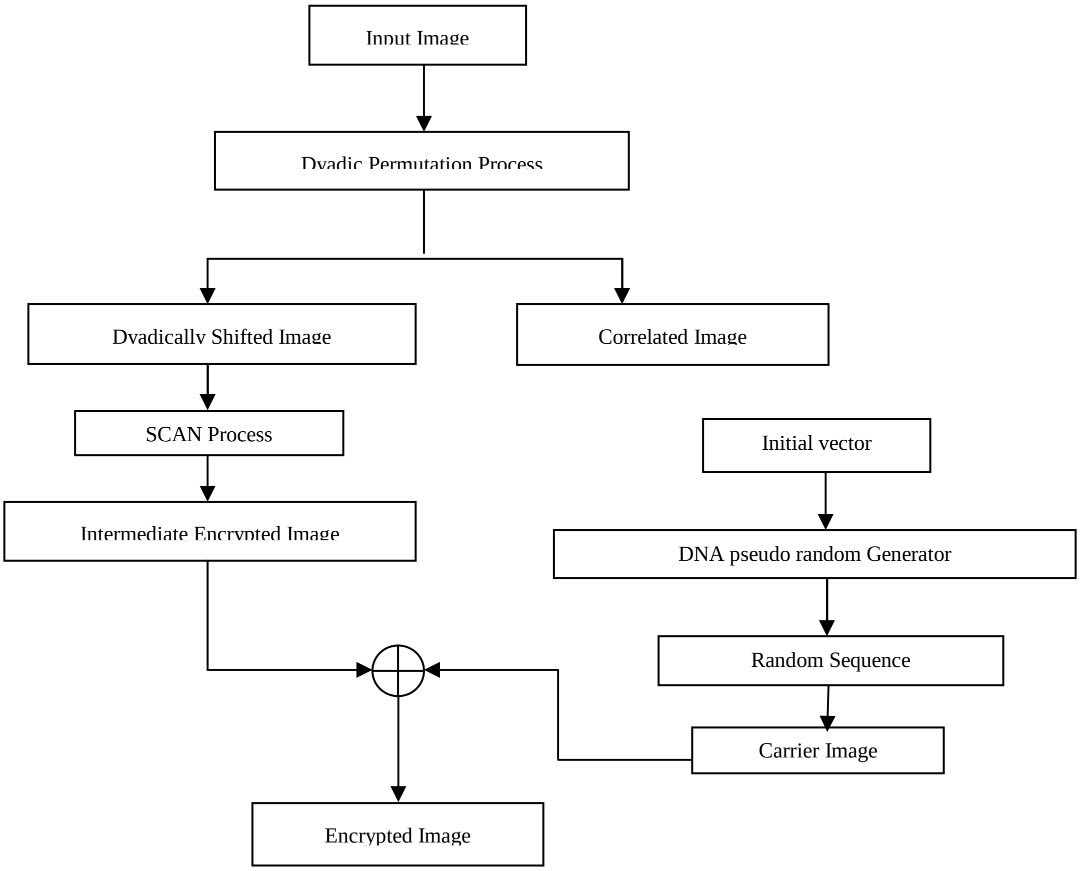


Fig. 2 Block diagram of the proposed system

In SCAN algorithm, first scan pattern is chosen by the user. The chosen scanning pattern is used as encryption key which is defined by an encryption specific SCAN language. The intensity values of an image along the scanning path are determined and one dimensional string is constructed. Finally, intensity values are written to the image using raster scan pattern and encrypted image is constructed.

A linear congruential generator (LCG) is an algorithm that yields a sequence of randomized numbers calculated with a linear equation. The sequence of random numbers is generated using the equation (1).

$$X_{i+1} = (a X_i + c) \bmod m \qquad (1)$$

Where 'm' is modulus m > 0,'a' is multiplier 0<a<m, 'c' is increment 0≤ c< m and 'X$_0$' is starting value 0≤ X$_0$ < m.

Pseudorandom sequence is generated using a linear congruential generator algorithm. The number in the pseudorandom sequence are mapped to four letters g, c, a and t. Finally, carrier image is constructed using the pseudorandom sequence by converting the number of pseudorandom sequence to binary string. Once the carrier image is constructed using pseudorandom sequence, encrypted image is constructed using carrier image and original image. Exclusive-or operation is performed between carrier image and original image.

The proposed algorithm is as follows.

Step 1: Read the input image of size M X N where M is the height and N is the width.
Step 2: Split the input image into chunks. First, decide the rows and columns to determine the number of chunks and then calculate chunk height and width. Finally, draw the image chunks.
Step 3: Choose two values j and k which are required to perform the exclusive-or (XOR) onto the addresses of a two dimensional function where j <2^N-1 and k<2^M-1. Next, XOR operation is performed on the addresses of the input image chunks. The new address should have the same number of bits as the former ones.
Step 4:Prepare the correlation matrix and draw the correlated image for all image chunks. Correlation matrix is generated using the Equation 2.

$$\Gamma_{fg}(j,k) = \sum_{n=0}^{2^n-1}\sum_{m=0}^{2^m-1} f(n,m)g(n \oplus j, m \oplus k) \qquad (2)$$

where $f(n,m)$ denotes original image two-dimensional digital function and $g(n \oplus j, m \oplus k)$ denotes dyadically shifted (permuted) function.
Step 5: Join the image chunks to form the intermediate encrypted image and also correlated image.

Step 6: The set of scanning paths are chosen by the user. The chosen scanning pattern is used as encryption key which is defined by an encryption specific SCAN language.
Step 7: Scan the intermediate encrypted image according to the chosen scanning pattern order and one dimensional array list of intensity values is constructed.
Step 8: Draw the encrypted image by setting the intensity values in the raster scan pattern order.
Step 9: Linear Congruential Generator algorithm is the pseudorandom generator used to generate the pseudo random sequence. Sequence is generated using the Equation 1.
Step 10: Map the sequence to the four letters g, c, a and t. A stands for Adenine, G stands for Guanine, C stands for Cytosine and T stands for Thymine. The numbers in the sequence are limited to base 4 number system.
Step 11: Twelve successive numbers in the sequence are selected and each number is converted to binary string. Twenty four bits of twelve numbers from the sequence are used for each pixel and carrier image is drawn.
Step 12: Finally, perform XOR operation between carrier image and input image which results in encrypted image.

EXPERIMENTAL RESULTS

The algorithm was applied on a JPEG image of variable size with different colors. The results of the proposed approach on sample images are shown in Fig.3. The original colored image is chosen as input to dyadic permutation algorithm as shown in the Fig. 3. The resultant intermediate encrypted file of the dyadic permutation process is shown in the Fig. 4(a) and the correlated image is shown in the Fig. 4(b).

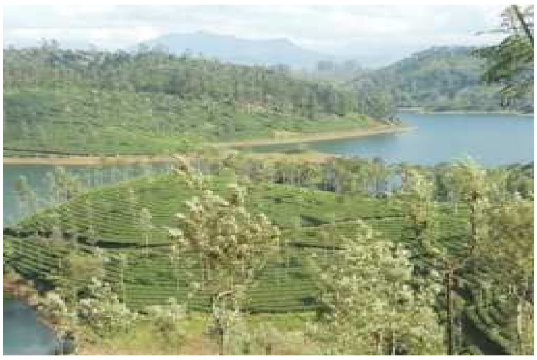
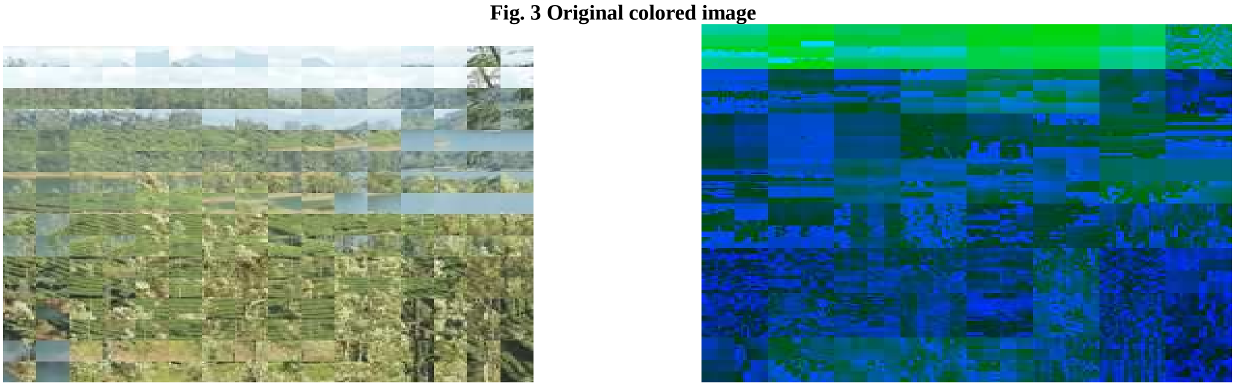
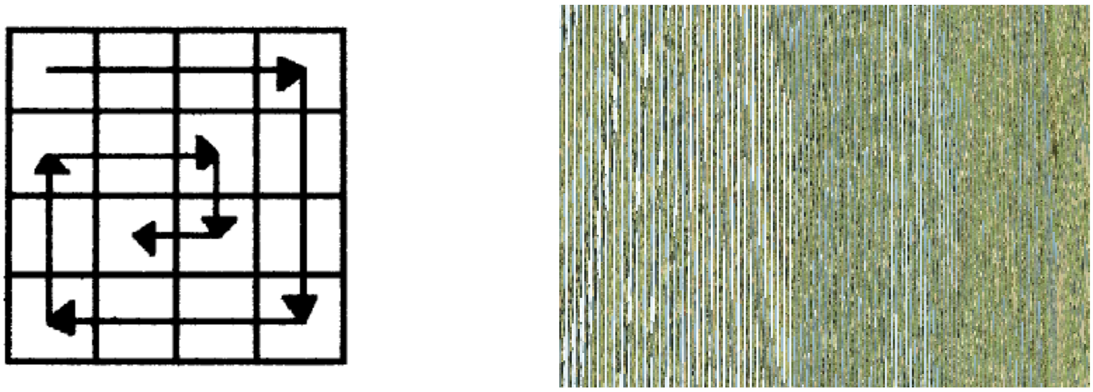


Fig. 3 Original colored image



(a) **(b)**

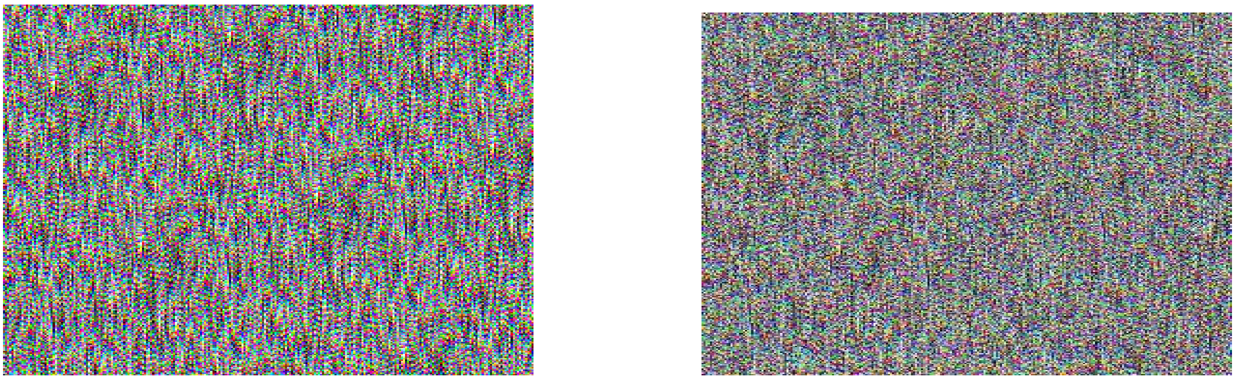
Fig. 4 (a) Cipher image after dyadic permutation process (b) Correlated Image



(a) **(b)**

Fig. 5 (a) Spiral Scan Pattern (b) Cipher image after SCAN process

In scan algorithm, firstly scan patterns are chosen by the user. Spiral scan pattern is shown in the Fig. 5(a). Next, based on the scan patterns image is scanned and image is encrypted. Encrypted image is shown in the Fig. 5(b). Carrier image is generated using the binary sequence. Sequence is generated using the Linear Congruential Generator algorithm (LCG) but the sequence numbers are limited to base 4 number system. Carrier image size is equal to the size of the original input image. Carrier image is shown in the Fig. 6(a). Carrier image and the intermediate encrypted image are XORed to form the encrypted image and shown in the Fig. 6(b). Decrypted image of the proposed system is shown in the Fig. 7.



(a) **(b)**

Fig. 6 (a) Carrier image (b) Final Encrypted Image

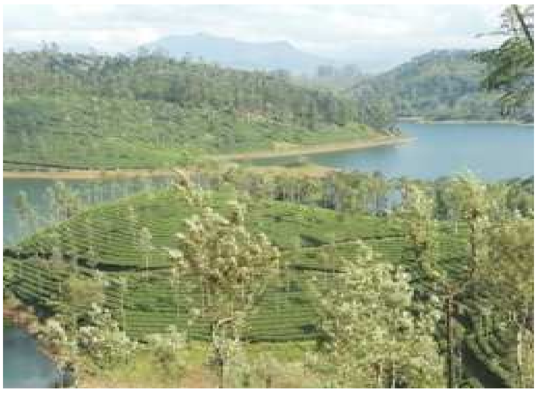


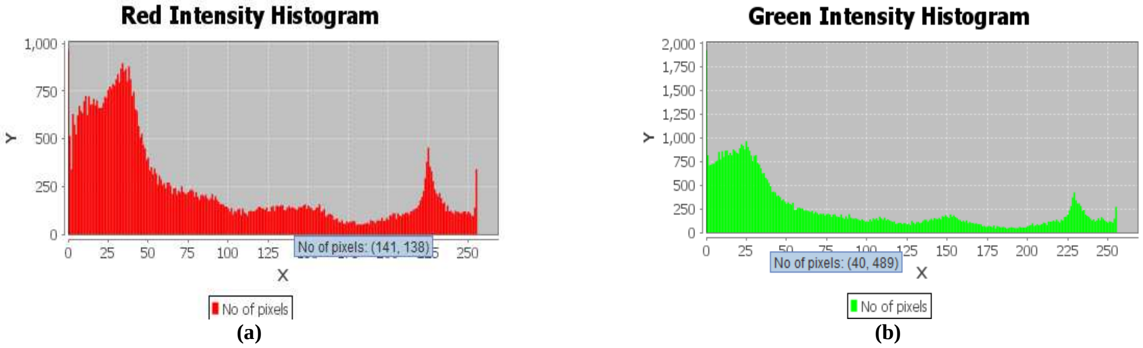
Fig. 7 Decrypted Image

STATISTICAL ANALYSIS

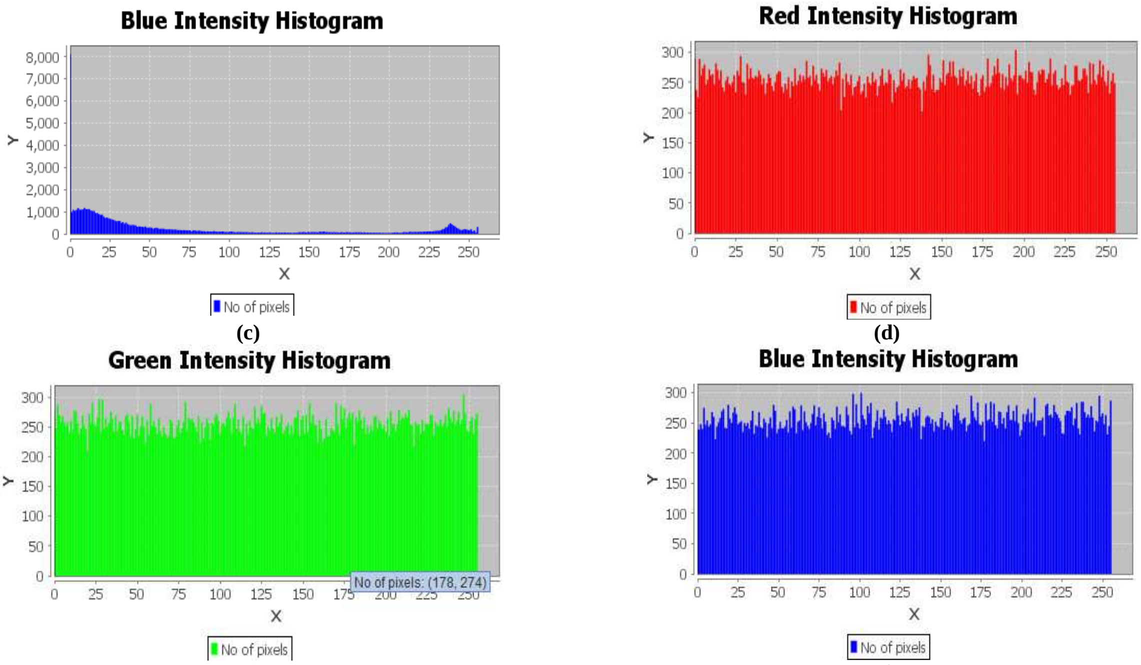
From the literature, it is known that many ciphers have been successfully analyzed with the help of statistical analysis. Further, several statistical attacks have been devised on them. To prove the robustness of the proposed method, statistical analysis is performed by plotting the histograms of the original and cipher images. The performance of the algorithm is measured in terms of correlation coefficient between original and cipher images.

Histogram Analysis

Histogram is plotted for original image and encrypted image as shown in Fig. 3 and Fig. 7 respectively. Histogram for the original image of the Fig. 3 is shown in Fig. 8(a), (b) and (c) of red, green and blue component respectively. Histogram for the encrypted image of the Fig. 7 is shown in Fig. 8 (d), (e) and (f) of red, green and blue component respectively. Histogram of the original image represents unequal occurrence of the colour components. But histogram for encrypted image shows that colour components are almost uniform. Occurrences of each pixel are uniform in the encrypted image.



(a) **(b)**



(c) (d)

(e) (f)

Fig. 8 Histogram of original and encrypted image

Encryption and Decryption Time

Table 1 summarizes the encryption/decryption speeds for encryption algorithm based on SCAN, dyadic permutation and carrier image. Comparative speed test results of the encryption algorithm on the input image as shown in the Fig. 3 are tabulated.

Table – 1 Speed Test Experimental Results of the Encryption Algorithms

Encryption/Decryption algorithm	Time taken for Encryption (Sec)	Time taken for Decryption (Sec)
Dyadic Permutation	5.68	0.2
SCAN algorithm	0.04	0.15
Carrier Image	0.5	0.94
Hybrid technique	6.28	1.03

Correlation Coefficient Analysis

Correlation between adjacent pixels in original image and their encrypted image is calculated. For an ordinary image, each pixel is usually highly correlated with its adjacent pixels. These high correlation properties can be quantified as the correlation coefficients for comparison. In Table 2, the results of correlation coefficients between the corresponding pixels of the plain input image have been delineated.

In this analysis 2000 pairs of adjacent pixels are selected from the image. Correlation values are shown in the Table 3. The correlation coefficient for plain image is 0.9. The horizontal and vertical coefficient of encrypted image generated using dyadic permutation and SCAN algorithm indicates that two adjacent pixels are of high correlation .The horizontal correlation coefficient is -0.06 and vertical correlation coefficient is 0.87 for cipher image encrypted using carrier image. The horizontal correlation coefficient is -0.01 and vertical correlation coefficient is 0.04 for cipher image encrypted using carrier image. In case of hybrid technique, the correlation coefficients for plain image with that of cipher images are far apart. The horizontal and vertical coefficient of encrypted image generated using hybrid technique indicates that two adjacent pixels are of low correlation among the algorithms listed in the Table 3.

Table - 2 Correlation Coefficients between the Pixels of Plain Input Image

Direction	Plain-image
Horizontal	0.90155
Vertical	0.95394

Table - 3 Correlation Coefficients between the Pixels of Encrypted Image

Encryption/Decryption algorithm	Horizontal	Vertical
Dyadic Permutation	0.86603	0.85261
SCAN algorithm	-0.04178	0.93161
Carrier Image	0.16584	0.04623
Dyadic Permutation + SCAN algorithm	-0.06355	0.87249
Dyadic Permutation + SCAN algorithm+ Carrier Image	-0.01358	0.04339

CONCLUSION

In this work, a new image encryption scheme based on SCAN, Dyadic permutation and Carrier image to encrypt and decrypt the image has been proposed. The main advantage of the proposed technique is it provides increased security. Dyadic algorithm adds security by scrambling the image using key and placement of key in correlated image. SCAN algorithm adds security by scrambling the image using scanning pattern as key. Since carrier image is generated using pseudo random numbers based on DNA sequence, it is not possible to predict the numbers without knowing the seed. Even a single change of bit in seed changes the carrier image and decryption is not possible. The result obtained is analyzed through histograms and correlation coefficient.. The analysis carried out reveals that the implemented system is working satisfactorily. The proposed system works well for still images. Encryption of video images is considered as further extension of the current study.

REFERENCES

[1] SS Maniccam and NG Bourbakis, Scan Based Lossless Image Compression and Encryption, *Proceedings of International Conference on Information Intelligence and Systems*, **1999,** 490-499.

[2] Roman Castaneda, Jorge Garcia-Sucerquia, Rodrigo Henao and Osvaldo Trabocchi, Information Encryption through Dyadic Permutation, *Opt and Laser in Eng*, **2001,** 36 (6)**,** 537-544.

[3] Qiang Zhang, Shihua Zhou and Xiaopeng Wei, An Efficient Approach for DNA Fractal-based Image Encryption, *Applied Mathematics & Information Sciences*, **2011,**5 (3), 445-459.

[4] BL Hao, HC Lee and SY Zhang, Fractals Related to Long DNA Sequences and Complete Genomes, *Chaos, Solutions & Fractals*, **2000,** 11 (6), 825–836.

[5] Rinki Pakshwar, Vijay Kumar Trivedi and Vineet Richhariya, Image Encryption Using Random Scrambling and XOR Operation, *International Journal of Engineering Research & Technology*, **2013,** 2 (3), 1-7.

[6] Panduranga HT and Naveen Kumar SK, Hybrid Approach for Image Encryption Using SCAN Patterns and Carrier Images , *International Journal on Computer Science and Engineering*, **2010,** 2 (2), 297-300.

[7] N Bourbakis and C Alexopoulos, A Fractal Based Image Processing Language - Formal Modeling, *Pattern Recognition Journal*, **1999,** 32 (2), 317-338.

[8] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering*, **2013,** 3 (6), 419-421.

[9] Petoukhov SV, Dyadic Groups, Dyadic Trees and Symmetries in Long Nucleotide Sequences, *http://arxivorg/abs/12046247*, **2013,** 1-43.

[10] Grasha Jacob and A Murugan, DNA Based Cryptography: An Overview and Analysis, *IJES*, **2013,** 3(1),36-42.

[11] Thomas H Frank, Implementation of Dyadic Correlation, *IEEE Transactions on Electromagnetic Capability*, **1971,** 13 (3), 111-117.

[12] Reza Moradi Rad, Abdolrahman Attar and Reza Ebrahimi Atani, A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR, *International Journal of Signal Processing, Image Processing and Pattern Recognition*, **2013,** 6 (5), 275-290.

[13] C Alexopoulos, N Bourbakis and N Ioannou, Image Encryption Method Using a Class of Fractals, *Journal of Electronic Imaging*, **1995,** 4 (3), 251-259.