International Journal of Electrical, Electronics and Computer Engineering **7**(1): 01-05(2018)

ISSN No. (Online): 2277-2626

A Image Encryption Scheme is Based on Scan Pattern for Colour Image

Satyam Pandey* and Prof. Amit Shrivastava**

**M. Tech. Scholar, Department of Electronics and Communication Engineering, VNS Faculty of Engineering, Bhopal (Madhya Pradesh), India*

***Assistant Professor, Electronics and Communication Engineering, VNS Faculty of Engineering, Bhopal (Madhya Pradesh), India*

(Corresponding author: Satyam Kumar Pandey)

(Received 15 December, 2017 Accepted 18 January, 2018)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: This encryption method is based on SCAN patterns generated by the SCAN methodology. The SCAN is a language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths. Then scanning paths sequence fill in original image. Note that the scanning paths with random code generating procedure, which produces the encryption keys in a very many ways; so come to the quite secret system. The encryption specific 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. Since most images require different scanning in different sub regions, the encryption specific SCAN language allows an image region to be recursively partitioned into four subregions and each subregion to be scanned independently. The partition patterns are letter B, letter Z, and letter X, each of which has eight transformations as previous mention

Keywords: Encrypted and Decrypted Image, Scan Image, specific SCAN language**,** transformations numbered.

I. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image security. Image encryption techniques try to convert original image to another image that is Hard to understand; to keep the image confidential between users, in other word, it is Essential that nobody could get to know the content without a key for decryption. The process of encoding plain text messages into cipher text messages is called encryption. And the reverse process of transforming cipher text back to plain text is called as decryption. Image and video encryption have applications in various fields Including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Colour images are being transmitted and stored in large amount over the Internet and wireless networks, which take Advantage of rapid development in multimedia and network technologies. In recent years, plenty of colour image encryption approaches have been proposed. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA most of which are used in text or binary data. It is difficult to use them directly in multimedia data and inefficient for colour image encryption because of high correlation among pixels. For multimedia data are often of high redundancy, of large volumes and require real-time interactions

II. OVER VIEW OF SCAN LANGUAGE

SCAN [11] is a class of formal languages, which can be applied to encryption, data hiding, compression, or combinations thereof. This section describes the SCAN language in detail [10] and provides some experimental results on the quality of the methodology obtained from the implementation of the algorithm in software

A scanning of a two dimensional array

$P_{m\times n}= \{p\ (i, j) :1 \le i \le m, 1 \le j \le n\}$ is a bijective function from $P_{m\times n}$ to the set $\{1,2,\ldots,mn-1,mn\}$.

In other word, 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. Note that an $n\times n$ array has $(n\times n)!$ Scanning.

The SCAN [5-7] is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths.

The SCAN is a family of formal languages such as Simple SCAN, Extended SCAN [10], and Generalized SCAN, each of which can represent and generate a specific set of scanning paths. Each SCAN language is defined by a grammar and each language has a set of basic scan patterns, a set of transformation of scan patterns and a set of rules to recursively compose simple scan patterns to obtain complex scan patterns.

Note that this set of basic scan patterns can be extended or reduced as needed by a specific application. There are six transformations of scan patterns. They are identity, horizontal reflection, and vertical reflection, rotation by 90, 180, and 270°, and compositions of these transformations. The rules for building complex scan patterns form simple scan patterns are specified by the production rules of the grammar of each specific language.

III. SCANNING OPERATION

A given image is encrypted by rearranging the pixel of the image using a set of scanning paths. This set of scanning paths is chosen by the user, and it is the encryption key. The scanning paths which are used as encryption keys are defined by an encryption specific SCAN language. For a given 2D $2^n \times 2^n$, image, the encryption algorithm transforms it into one dimensional strings of length 2^{2n} firstly. Then each arrangement strings of length are encrypted using random generating encryption keys. Fig. 1 shows how we encrypt a 4×4 image. Transform one-dimensional string of length 16 using an encryption key. Then wide string data according filled the new 4×4 encryption image.

IV. LOGIC OF ENCRYPTION

Following by basic scan patterns and partition patterns to produce concept, we use a random code generating produce the SCAN word and to define encryption key. The SCAN word contain scan and partition patterns. The scan partition word has c0~c7, d0~d7, o0~o7 and s0~s7. The partition word has B0~B7, Z0~Z7 and X0~X7. This word separately had done specially scanning paths and partition. Because the SCAN word has large variation, so we can attain encryption technology. Consider the 16×16 size image and the scanning path shown in Fig. 1. The scanning path is corresponding to the SCAN word [2] constructed as follows. The SCAN word shown in figure1 a defines encryption key can achieve encryption objective

1 Take original image
2. Determine image in size of $2^n \times 2^n$
3. Analysis Latter and Number of partition pattern for each
4. Partition Letter ϵ{B, Z, X} and for each transformation
   Number ϵ 0, 1, 2, 3, 4, 5, 6, 7
5. Determine did what partition pattern
6. If Letter =’B’ Perform Letter B pattern
7. If Letter =’Z’ Perform Letter Z pattern
8. If Letter =’X’ Perform Letter X pattern
9. Now we will get Partition image in four segments

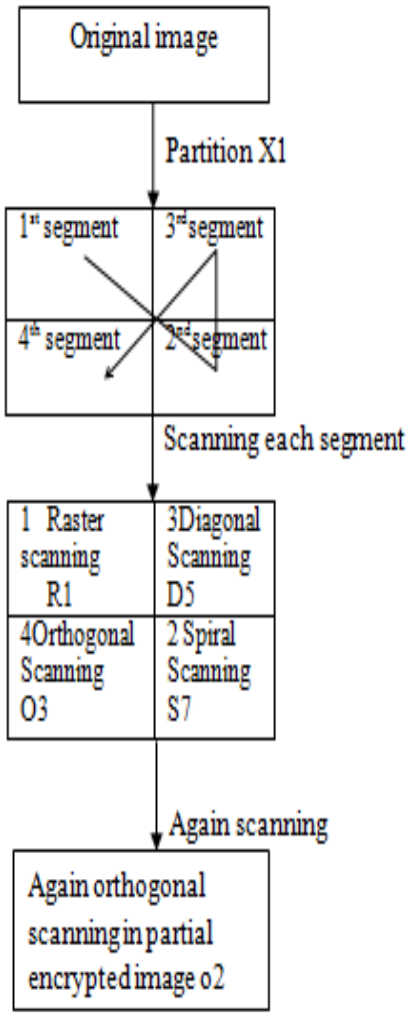


Fig. 1. The SCAN word diagram.

V. SCAN ALGORITHM

1. Take Image
2. Determine image in size of $2^n \times 2^n$
3. Analysis Latter and Number of scan pattern for each
   Scan Letter ϵ{c, d, o, s} and for each transformation Number ϵ 0, 1, 2, 3, 4, 5, 6, 7
4. Determine did what scan pattern
5. If Letter =’c’ Perform continuous raster c pattern
6. If Letter =’d’ Perform continuous diagonal d pattern
7. If Letter =’o’ Perform continuous orthogonal o pattern
8. If Letter =’s’ Perform spiral s pattern
9. Produce 1×2^{2n} scanning paths image and deliver to image out.There are many encryption method exist.

They inlude scan based method, chaos based methods, structure based method, double random grid etc.

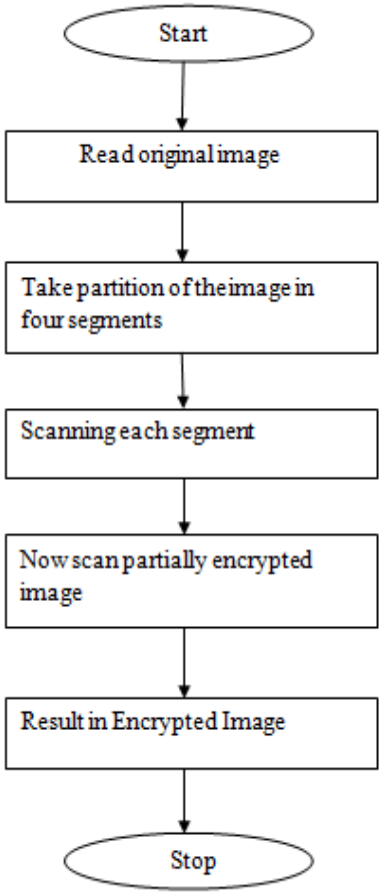


Fig. 2. Flow chart for proposed Encryption method.

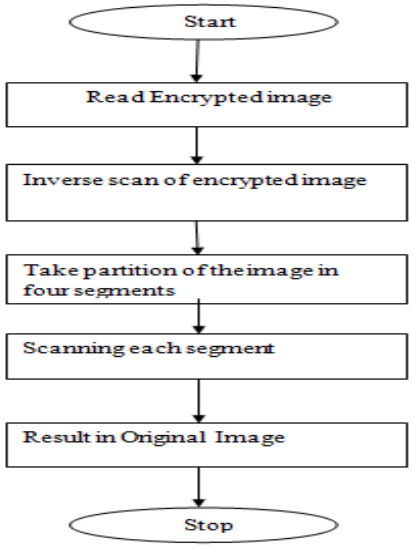


Fig. 3. Flow chart for proposed Decryption method.

However each of them has its strength and weakness in terms of security level and processing speed. Some of them have high security level but less processing speed and some of them high processing speed but less security level. To overcome above mentioned problem we proposed new modified SACN algorithm to encrypt the image.

VI. PROBLEM IDENTIFICATION

The SCAN algorithm is newly approach of image security. In this method encryption key is generated directly through partition and scanning path. It has high security level and high processing speed. As it has been noticed in the base paper "Image encryption and decryption by using SCAN methodology" has low security level on account of very easily predicted to see encrypted image which algorithm is applied and how many partition are over there .For Different Scan Patterns

A-Result Encrypted and Decrypted Images

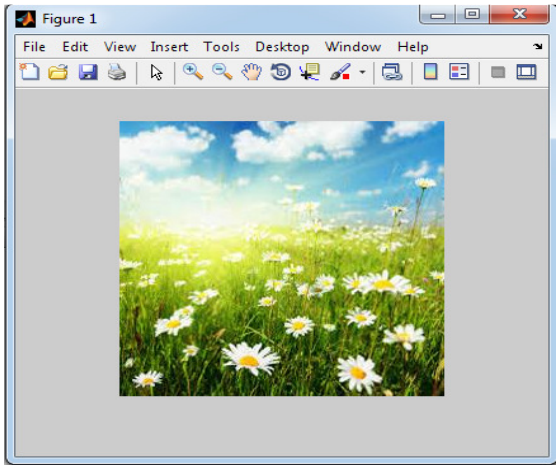


Fig. 4. Original sun flower image.

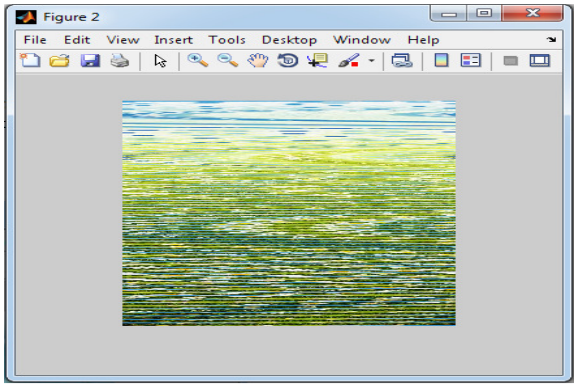


Fig. 5. Encrypted image by orthogonal scanning.

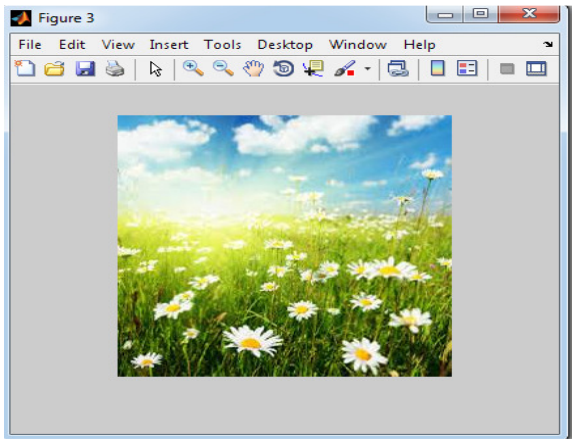


Fig. 6. Image after decryption by orthogonal scanning

B. Encrypted and Decrypted Images Based on Proposed Method

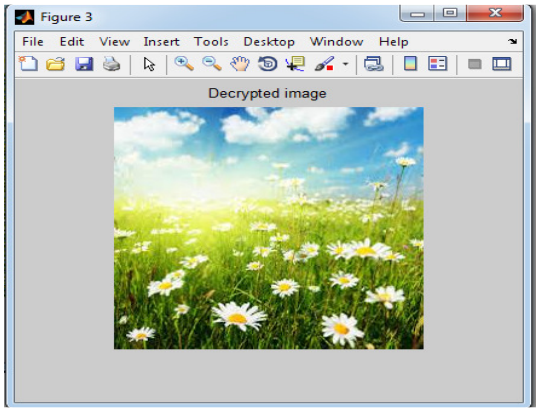
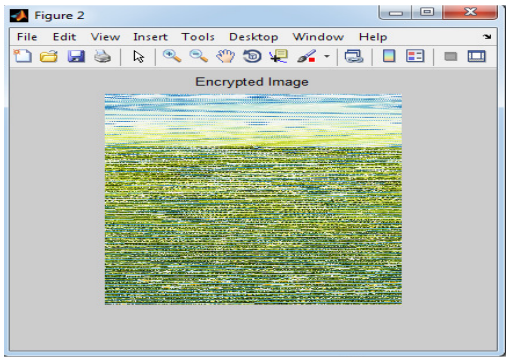


Fig. 7. Encrypted Image by proposed method.



Correlation Factor = 0.1362, Execution Delay = 5 seconds

VII. SECURITY ANALYSIS

Security analysis can be performed with the help correlation factor. Its value varies from 0 to 1. If it is 1 both plain image and cipher image same and if 0 it has no similarity.

Correlation factor of previous and proposed which is shown in table 1. As correlation factor of proposed method is less with previous method so it gives better security with less execution delay.

Table 1: Comparison between Previous Method and Proposed Method.

Sr. No	Previous Method	Proposed Method
1	This is implemented for gray scale image	This is implemented for color scale image
2	It takes high execution delay (15 to 18 seconds).	It takes small execution delay (5 to 9 seconds).
3	It gives low security crypto image. Security can be compared with the help of correlation factor.	It gives high security crypto image.
4	It has variable length of key space depends on image size.	It has fix length of key space depends on image size.
5	The combination of encryption key is depends on the image size. Large combination is possible for large image.	It also has millions of combination of encryption key.(8 * 8* 8 * 8 * 8 * 8 * 8 = 2097152). It is free from image size.

Table 2: Correlation factor & Execution Delay for Previous Method and Proposed Method.

Sr. no.	Image	Correlation Factor		Execution Delay	
		Previous Method	Proposed Method	Previous Method	Proposed Method
1	Sun Flower Image(256×256)	0.3142	0.1362	11	5
2	Image(512×512)	0.3213	0.2162	14	8
3	Standard (Lena) Image(256×256)	0.2231	0.1862	12	6
4	Medical Image(512×512)	0.2149	0.1746	15	7

VIII. CONCLUSION

This revolutionary age of the multimedia and networks making employing of more and more images and transmission among the computer systems. The image security is of substantial vitality now a days. If previous method is compared, the security is enhanced which has been shown in the result. The security is furthermore added up by scanning whole image after performing scanning for each segment.

Therefore the resultant encrypted image appears to be single image and the process of encryption is almost unpredictable. The proposed encryption method can achieve two goals. One is to design highly secured image cryptosystem. The other is to reduce the time for encryption and decryption. There are many features of the SCAN methodology such as Lossless encryption of image, increased Security by the use of more several encryption loops.

REFERENCES

[1]. M. Sivagami,R. Premkumar, S. Anand. An efficient method based on crossover operator for image encryption 7-18 March 2017 DOI: 10.1109/ICIIECS.2017.8276176 IEEE.

[2]. S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2016 International Conference on Electronics and Information Engineering (ICEIE 2010).

[3]. Z. Yun-peng , Z. Zheng-jun "Digital Image Encryption Algorithm Based on Chaos and Improved DES "Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2015.

[4]. K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 ©2006 IEEE.

[5]. Paul A.J P. M. K. Paulose Jacob "Matrix based Cryptographic Procedure for Efficient Image Encryption.

[6]. H. Gao, Y. Zhang, S. Liang, D. Li "A New Chaotic Image Encryption Algorithm "Chaos, Solitons and Fractals, **29** (2006) 393–399.

[7]. A. Gautam, M. Panwar, Dr. P.R Gupta "A New Image Encryption Approach Using Block Based Transformation Algorithm" 2005 *(IJAEST)* Vol. No. **8**, Issue No. 1, 090 – 096.

[8]. Q.Hua Lin, Fu-Liang Yin, and Y.R. Zheng" Secure image communication using blind source separation" 2004 IEEE.

[9]. R. Y. H. Zhao "An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps" I. *J. Computer Network and Information Security*, 2012, 7, 41-50.

[10]. R. liu, X. tian "New algorithm for color image encryption using chaotic map and spatial bit level permutation" *Journal of Theoretical and Applied Information Technology* 15 September 2012. Vol. **43** No.1 2005 - 2012 JATIT & LLS.