International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT11953131

Secret sharing scheme Circular Visual Cryptography for Color Images

Sudhir Parmar[1], Dr. Sheshang D. Degadwala[2]
[1]PG Scholar, Computer Engineering Department, Sigma Institute of Engineering, Vadodara, Gujarat, India
[2]Head of Department, Computer Engineering Department, Sigma Institute of Engineering, Vadodara, Gujarat, India

ABSTRACT
Data security is the most significant part of the innovative work territory, government, industry, association, and so forth. As of late, cybercrime or related hacking issue increments to an ever-increasing extent. So high security is required to verify the data as well as the picture. Visual Cryptography Scheme (VCS) is one of the procedures to verify the data utilizing straightforward calculation while in some other security method complex calculation was utilized. VCS has a straightforward encryption calculation which is secure data changing over into the various offers and for the unscrambling procedure don't require any kind of gadgets or any mind-boggling decoding calculation. The unscrambling procedure is finished utilizing the Human Visual Scheme (HVS). Round Random Grid offers are superior to the rectangular offers since usefulness is expanded by secure various data in the roundabout irregular network to give the secrecy. In the proposed plan, mystery sharing plan is that mystery data is separated into different importance full and negligible offers and is additionally recouped by superimposing handling and it is seen by HVS. In this Research, we depict each technique for VCS and introduced its relative investigation utilizing points of interest and hindrances.

Keywords : Random Grid, Secret Sharing Scheme, Visual Cryptography Scheme (VCS), Circular Grid, Random Grid

I. INTRODUCTION

To get the improvement in the existing framework that gives high protection from the programmer, the proposed framework will apply to verify the data. Presently a day's cybercrime is at top position which is a challenge for up and coming exploration. Along these lines, to give the security to private information is a prime require Random Grid, Secret Sharing Scheme cement.

In the present innovation, the war of ensuring classified information is going extraordinary by 60 minutes. Numerous strategies have been created to conquer the cybercrime-related issue, for example, Cryptography and picture steganography. These are the great plan where the previous needs uncommon unscrambling gadget and the last never uncovers its essence.

Cryptography is a procedure of encryption and decoding both. Encryption implies unique content, data or pictures changed over into figure content or in muddled structure. The unscrambling procedure is the turnaround of the encryption procedure. However, in customary cryptography, encryption and decoding procedure is finished by the key. Also, the key is the either symmetric or uneven calculation. So in cryptography procedure opportunity to lessen the security [8].

Visual cryptography is another system and assuming a virtual job the extent that the present security needs are concerned. In the Visual

Cryptography Technique when there is a more pixel extension then the visual nature of the resultant picture is corrupted just as it gives an extremely huge recreated picture which is undesired.

In visual cryptography mystery picture changed over in to no. of offers structure and these offers dispersed into the no. of members, this is the encryption procedure and unscrambling procedure is finished by Human Visual System (HVS) in any event, when commotion is incorporated into any reassemble picture, no prerequisite of a gadgets and complex algorithm[1]. This procedure is more secure than the cryptography strategy.

The greater security level is expanded by the Circular VCS Scheme. To verify Binary, Gray and Color Image with proposed Circular Random network-based Visual Cryptography. To Divide the picture into (k, n) Share Scheme (for example 2, 4, 8, 16) Using Hierarchical Circular Visual Cryptography. To improve the PSNR and MSE estimation for Recover information.

In (k, n) limit model, create then no. of offers and disseminated in the members. On the off chance that members join not as much ask or k-1 offers, at that point can't extricate mystery picture. On the off chance that and just in the event that consolidates all the investment or k offers, at that point and afterward separate the first mystery picture. Generally unrealistic to separate the first mystery picture. So in the way expands the security level of the mystery pictures and/or data.

II. RELATED WORKS

M. Chakravorty and S. Gurung [1], in this paper proposed framework, is, strategy to conceal the various mystery data in a couple of offers and utilize the QNN to improving the security of the mystery data and General Access Structure (GAS) is utilized to shroud the information. The approach is Circular irregular Grid, different data is concealing utilizing the roundabout arbitrary framework or round offer. To address the issue of rakish pivot by the roundabout irregular network since roundabout lattice turns at the different edge to shroud the numerous data. What's more, no pixel extension issue is produced in this strategy. QNN is utilized to extricate the first data structure the roundabout offers in any event when data isn't obviously unmistakable and the QNN system won't be tapped at any neighborhood minima. In this paper encode the different data into the round offers and unscramble by the Human Visual System (HVS).

Z.- R. La and X. Wu[2], in this paper to address the pixel extension issue and to give the adaptable sharing technique. In the proposed technique pixel extension for the diverse limit is constantly 1, in different strategies when the estimation of k and n is increment pixel development of strategy increases. To address the above issue RG-CBW-VCS calculation is utilized for GAS and XOR activity is applied to the shading pixel. Further stretches out the proposed framework to understand the Generalized General Access Structure (GGAS), in GGAS enables the clients to allocate various probabilities to the distinctive insignificant qualified sets. These proposed frameworks demonstrated by utilizing the various Lemmas and Theorems. Likewise, demonstrate the hypothetical and exploratory estimation of the security and differentiation condition whether the two qualities are close by or not.

C.- N. Yang and X. Wu [3], in this paper proposed plan is the blend of the CBW-VCS and Polynomial based Secret Image Sharing (PSIS). Shading share age is likewise a proposed framework. In this paper incorporates two decoding process: stacking-to-see and lossless picture remaking. XOR activity is utilized to improve visual quality. Dim scale mystery picture is converted into the p-radix picture and twofold picture and afterward encode p-

radix picture by (k, n) PSIS under mod p (in this paper creator taking p = 19) activity. For the ideal recuperation of the p-radix picture is finished by utilizing Lagrange polynomial insertion strategy and double picture review unscrambling is finished by stacking. The hindrance of the proposed strategy (mix of CBW-VCS and PSIS) is to marginally decrease the nature of the recouped picture contrasted with the ordinary VCS.

R. N. Chaturvedi et al. [5], in this paper proposed approach, is to improve the quality, differentiate level, resize the recouped mystery picture and to diminish the clamor which is available in the reproduced picture. In this paper MSE, PSNR and SSIM parameter is utilized to gauge the exhibition of the unique picture and reassembled picture. In this paper, two strategies are utilized to resize the recreated picture one is direct interjection and the second is safeguard the segment and line (1 out of n). Technique 1 gives the normal estimation of the MSE, PSNR, and SSIM and strategy 2 gives the definite estimation of the parameter. In this paper get the perfect estimation of MSE, PSNR, and SSIM for paired, dark and shading pictures, MSE as"0", PSNR as "boundlessness", and SSIM as "1".

A. Gupta and A. Mishra [8], in his paper proposed framework, is (2, n, m) multi mystery sharing plan in this plan n offers are created to shroud them mystery pictures and proposed calculation depends on stacking of offers. Least two offers are required to decode one mystery picture, for example, m+1 or n offers are required to recuperate unique mystery picture. Pictures are recuperated just when offers have a place with the certified sets on the off chance that offers has a place with taboo sets, at that point can't be conceivable to reproduce the unique picture. Picture reproduction is finished by superimposing these offers. In this paper to address the arrangement issue at the time of decoding by utilizing XOR activity.

1.1 DIFFERENT METHODOLOGIES

A. VISUAL CRYPTOGRAPHY SCHEME (VCS):

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted using an encoding system that can be decrypted by eyes. It does not require a computer for the decoding.

Types of VCS: (2, 2) VCS, (K, N) VCS, (N, N) VCS

Theoretical Background: Traditional VCS, Random Grid VCS and XOR based VCS

1. TRADITIONAL VCS:

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system.

The secret image (a) is encoded into (b) & (c) two shares and (d) is decoded by superimposing these two shares with 50% loss of contrast.

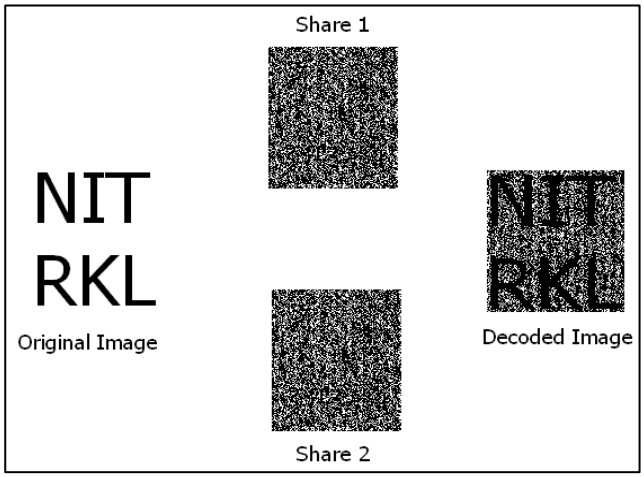

Figure 1 : Example of a two-Out of-Two VCS

2. RANDOM GRID VCS:

A random grid encrypts the secret information into 2D arrays of transparent and opaque pixels. The scheme is simple and does not involve any increase in pixel size. Whatever problem is present

Traditional VCS same problem is present in random grid VCS.

B. CIRCULAR VISUAL CRYPTOGRAPHY SCHEME:

1. QNN

Quantum neural network (QNN) is a modified network of the Hopfield neural network and QNN gives multiple outputs levels. QNN is based on the local minima escaping capabilities. In general, each Q'tron is self -connected with negative connection strength to provide means for negative feedback. To extract the original information with the help of the QNN even when the information is not clearly visible to the human eye.

2. CIRCULAR RANDOM GRID VCS

In this method there are two circular shares are required to hide the multiple images. One image is hide in these two circular shares and then any one circular share rotate at various angle and hide more than two secret images. No pixel expansion problem is generate in circular random grid VCS, hide the multiple information and no complex codebook is required. With the help of this methodology, both confidentiality and authentication can be achieve.

PROPOSED SYSTEM WORK

Proposed system is for three types of Images such as Binary Image, Grey Scale Image and Color Image. In proposed system general approach is to convert the any image into the circular grid and then generates a circular shares of that circular grid image using circular random grid method after the Completion of encryption process starts the decryption process. In decryption process combines the circular shares and generates the original image.

In this proposed system first extract the R, G and B component from the color image. This component acts as binary image then system read this binary image and resize it then generate a grid i.e. square color image into circular form. Apply the Random grid Circular Visual Cryptography (RCVCS) on the binary image to generate the shares (S1 Grid and S2 Grid). Two grid for the R component, two grid for the G component and two grid for the R component.

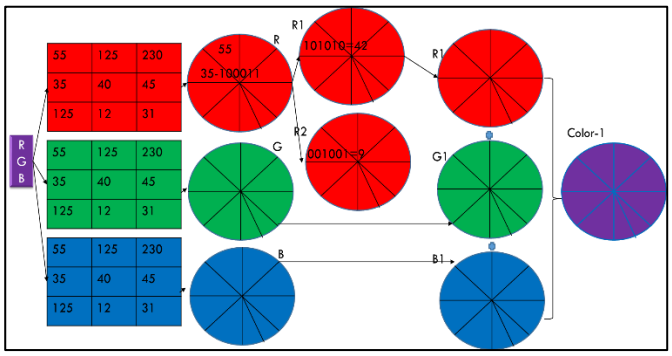

Figure 2 : Block Diagram for Color Image

After share generation process combine one grid R1 of R component, one grid G1 of G component and one grid B1 of B component and getting one common gird S11. Repeat same process for another grid and getting another new grid S22. This whole process is encryption process after completion of encryption process start the decryption process, in decryption process again extract the component and combine the grid shares and get the original color image.

III. RESULTS ANALYSIS

Result of the Random grid Circular Visual Cryptography algorithm for color image. Value of the PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Value). Reconstructed image is depending on the PSNR. PSNR value is high, quality of the reconstructed image is also high.

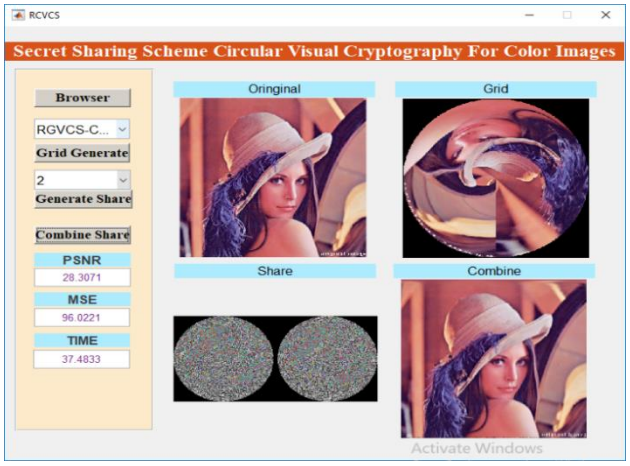

Figure 3: Results of Color Image 2-share

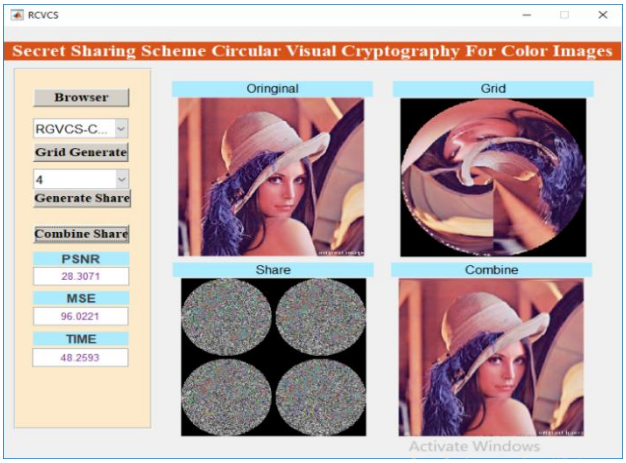

Figure 4: Results of Color Image 4-share

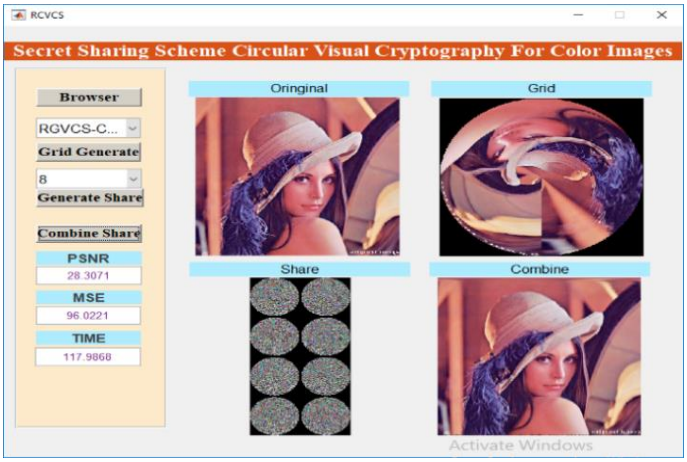

Figure 5: Results of Color Image 8-share

Table I: Comparative Analysis

Datasets	**No of Shares**								
No of Shares	2			4			8		
Parameters	PSNR	MSE	Time	PSNR	MSE	Time	PSNR	MSE	Time
Lena	28.3	96.022	37.48	28.31	96.02	48.25	28.3	96.2	117.98
Book	29.22	77.79	24.95	29.22	77.79	90.69	29.22	77.79	117.23
Earth	30.89	52.96	33.46	30.89	52.96	86.61	30.89	52.96	91.03
Cup	29.85	67.25	24.57	29.85	67.25	45.32	29.85	67.25	88.92
Office	26.17	156.79	121.45	26.17	156.79	279.11	26.17	156.79	336.06

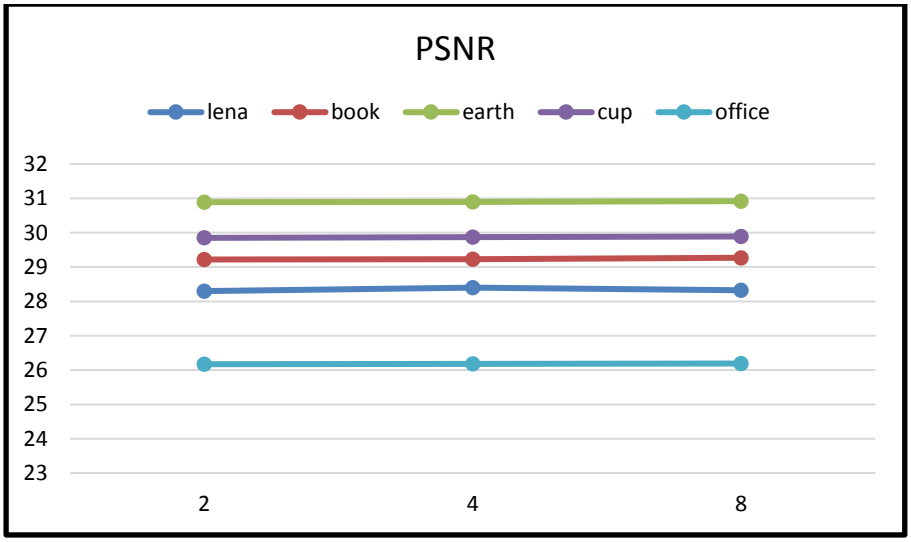

Figure 6: Analysis of PSNR Color Proposed System

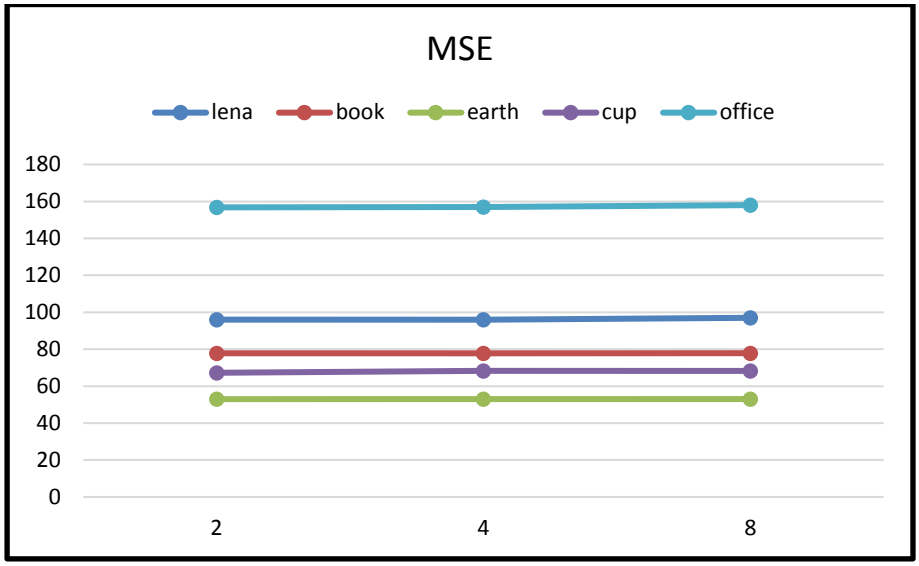

Figure 7: Analysis of MSE Color Proposed System

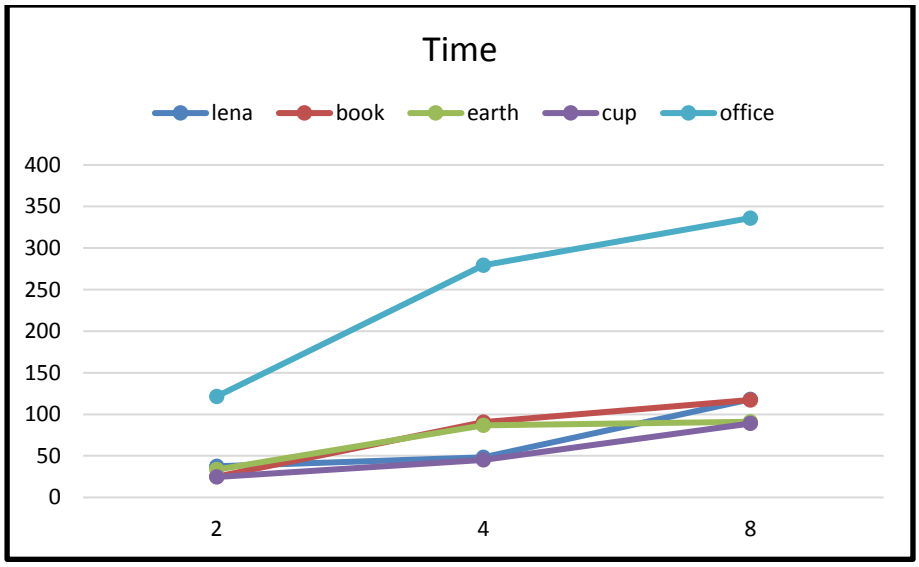

Figure 8: Analysis of Time Color Proposed System

IV. CONCLUSION

As Circular Shares are generated in hierarchical form using Proposed Color Random Grids Pixel Expansion algorithm. The mechanism achieves confidentiality of data and authentication of the end users. The System is work with Color images, Binary, and Gray Scale. As the shares are generated in (2, N) Scheme for increase security level. PSNR and MSE parameters shows that, when in proposed system generate more Shares the recover Image quality will not decrease. Proposed also works batter for any Color Images.

V. REFERENCES

[1]. Sandeep Gurung and Mrinaldeep Chakravort "Multiple Information Hiding in General Access Structure Visual Cryptography Using Q'tron Neural Network". Springer Nature Singapore Pte Ltd. Springer - 2018

[2]. Abhishek Mishra &Ashutosh Gupta "Multi secret sharing scheme using iterative Method". Journal of Information and Optimization Sciences - 2018

[3]. Bibhas Chandra Das, Md Kutubuddin Saradr, AvishekAdhikari "Efficient Constructions for t-(k; n)-Randon GridVisual Cryptographic Schemes".Institute of Electrical and Electronics Engineers (IEEE) - 2017

[4]. Tzung-Her Chen ,Kuang-Che Li "Multi-image encryption by circular random grids".International Conference on Intelligent Computing, Communication & Convergence Elsevier - 2009

[5]. Sandeep Gurung, Mrinaldeep Chakravorty, Abhi Agarwal, M K "Multiple Information Hiding using Circular Random Grids".International Conference on Intelligent Computing, Communication & Convergence Elsevier - 2015

[6]. Sandeep Gurung, BijoyChhetri, MrinalKantiGhose "A Novel approach for Circular Random Grid with Share Authentication".Institute of Electrical and Electronics Engineers IEEE - 2015

[7]. S. D. Degadwala and S. Gaur "4-Share VCS Based Image Watermarking for Dual RST Attacks". Springer International Publishing AG Springer - 2018

[8]. Shyong Jian Shyu " Visual Cryptograms of Random Grids for General Access Structures". Transactions on Circuits and Systems for Video Technology, VOL. 23 (IEEE) - 2012

[9]. Sandeep Gurung,Gaurav Ojha,M K Ghose " Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding". International Journal of Computer Applications VOL. 86 - 2014

[10]. Sandeep Gurung, Mrinal deep Chakravorty, Abhi Agarwal, M K Ghose "Multiple Information Hiding using Circular Random Grids".International Conference on Intelligent Computing, Communication & Convergence Elsevier - 2015

[11]. Pallavi Vijay Chavan, Dr. Mohammad Atique, Dr. Latesh Malik "Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography". Institute of Electrical and Electronics Engineers (IEEE) - 2015

[12]. Hsien-Chu Wu, Chin-Chen Chang "Sharing visual multi-secrets using circle shares" International Conference on Intelligent Computing, Communication & Convergence Elsevier - 2005

[13]. Xiao-Yi Liu, Ming-Song Chen, and Ya-Li Zhang "A New Color Visual Cryptography Scheme with Perfect Contrast".International Conference on Communications and Networking in China CHINACOM - 2013

[14]. Young-Chang Hou "Visual cryptography for color images".International Conference on Intelligent Computing, Communication & Convergence Elsevier - 2012

[15]. Thomas Monoth, Babu Anto P "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns".International Conference on Cyberworlds-2010

Cite this article as :

Sudhir Parmar, Dr. Sheshang D. Degadwala, "Secret sharing scheme Circular Visual Cryptography for Color Images", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 1316-1323, March-April 2019.

Available at doi :

https://doi.org/10.32628/CSEIT11953131
Journal URL : http://ijsrcseit.com/CSEIT11953131