Multi Reduce Permuted Share Visual Cryptography Technique

[1]Samiksha, [2]Kirti Bhatia, [3]Rohini Sharma*
[1]Student, [2]Assistant Professor, [3]Assistant Professor
[1]Sat Kabir Institute of Technology and Management, Bahadurgarh, India
[2]Sat Kabir Institute of Technology and Management, Bahadurgarh, India
[3]A.I.J.H.M. College, Rohtak, India
*Corresponding Author: Rohini Sharma

Abstract: Visual Cryptography is an exceptional encryption technique to conceal information in images in such a way that it can be decrypted by the human visualization if the correct key image is utilized. Visual cryptography (VC) is a way of protecting the secret image which encodes the image into various shares and distributes them to various members. In k out of n (k, n) method, the secret image is allocated into n shares such that when k or more members by assembling their limpidity through an overhead projector to divulges the secret image. This work proposes a novel, simple and hard to decode (k, n) visual cryptography procedure which is used to successfully sharing the secret image with extreme concealment. We have used permutation for n share, so that it becomes impossible for an outsider or attacker to decrypt the message encoded in an image.

***Index Terms* – Visual Cryptography, Share, Permutation, Encryption, Decryption.**

I. INTRODUCTION

The Visual cryptography technique was proposed by Naor and Shamir in 1994 [1]. Visual Cryptography permits information in the form of images, text and diagrams to be encrypted via an encoding structure that can be decrypted by the eyes. Computer is not needed to decode the information. The main idea behind this technique is to overlay two semi-transparent layers of an image. It is a visualization of two pieces of transparency protected with an apparently random throng of black pixels. **Figure 1** (a and b) shows two sheets of transparencies of an image.

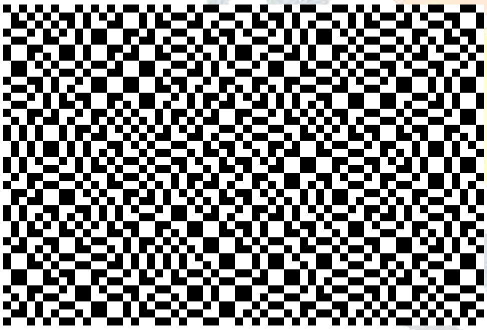


Figure 1 a: Sheet 1

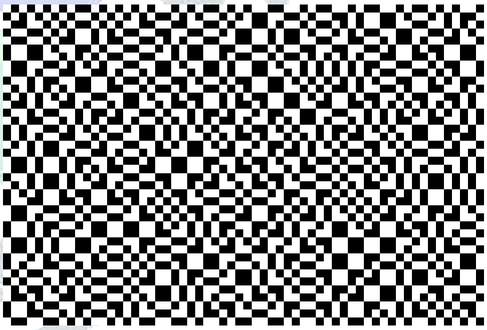


Figure 1 b: Sheet 2

Independently, there is no visible message printed on any of the sheets. Overlapping the sheets creates accumulating interference to the light passing through the sheets. It is like accomplishment of a Boolean OR operation on the images; however it just looks like a random assortment of pixels. If the two grids are overlapped properly, at appropriate position, a message appears. A monochrome image of the source is captured and the pixels in this image are black and white. These pixels are further subdivided into smaller pixels. These smaller pixels are shaded to create the source image. We need to scatter the shading in such a way that, if a person have one of the cypher images, it is unfeasible to decode the other cypher image.

II. RELATED WORK

Authors in [2-4] have defined various advanced cryptography techniques to solve different types of problems. Authors in [5] have given the FEAL algorithm for image encryption. It is a block cipher DES encryption scheme. They used 12 keys to encrypt an image of 12 X 12 blocks. Authors in [6] have provided scopes and challenges in the visual cryptography. Image can be encrypted by two means, with compression and without compression. Authors in [7] have used Quasi group compression technique to encrypt an image. The encrypted image is compressed gradually in resolution by Resolution Progressive Compression (RPC) technique. Quasi group techniques are mainly used for encryption during transmission. The wavelet based image compression reduces the amount of storage needed for encryption [8]. There is a considerable research work available in the field of image encryption [9-12]. Image encryption can be used in security procedures like secretly face recognition [13-14] of a suspicious person. It can also be used in the field of the wireless sensor networks [15-23], in the field of wireless body area networks [24-25] and in the field of energy holes problems [26-27].

III. Working of Visual Cryptography

Every pixel of the source images is partitioned into smaller blocks. The number of white (transparent) and black blocks is always same e.g. if a pixel is divided into two shares, there are one white and one black block. If the pixel is divided into four equal shares, there are two white and two black blocks.

In the figure 2, [28], a pixel is divided into four shares, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the over-layed pixel will be half black and half white. Such over-layed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the over-layed version will be completely black. This is an information pixel.

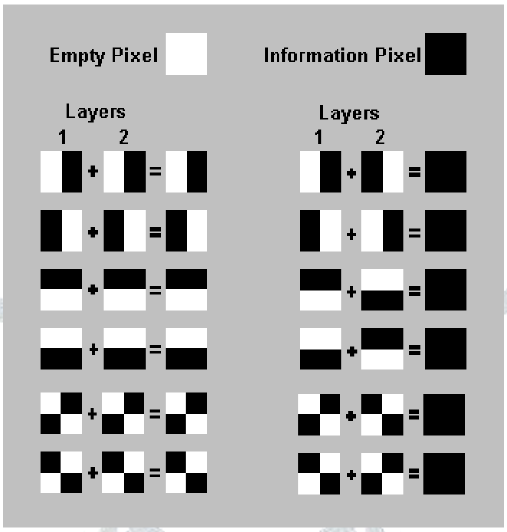


Figure 2: Pixel Combination

IV. Multi Reduce Permuted Share Visual Cryptography Technique

When all shares of an image are ranged and arranged together, they uncover the secret image. In k out of n (k, n), the secret image is shared into n shares such that when k or more participants by amassing their transparencies by means of an overhead projector to reveals the secret image. In share creation process, specified new condition for random matrices and then permutation operations are performed to generate the `n' transparencies. It is possible to decode the secret image visually by superimposing a k subset of transparencies.

Multi-Reduce permutation performs permutations of the columns and rows of an image to divide it [29]. First all the even-numbered columns are moved to the left half, while all the odd-numbered columns are moved to the right half. Then the same thing is done to the rows and the process is reiterated as shown in **Fig 3**. When the same permutation is employed to an image again and again, the initial image finally is formed. The number of permutations required to obtain the original image is called its period. The volume of an image intensely affects the period. For square images, the period increases, on average, with the volume. E.g., the period for a 100 X100 pixel image is 30, but for a 128 X 128 pixel image, it is 7.

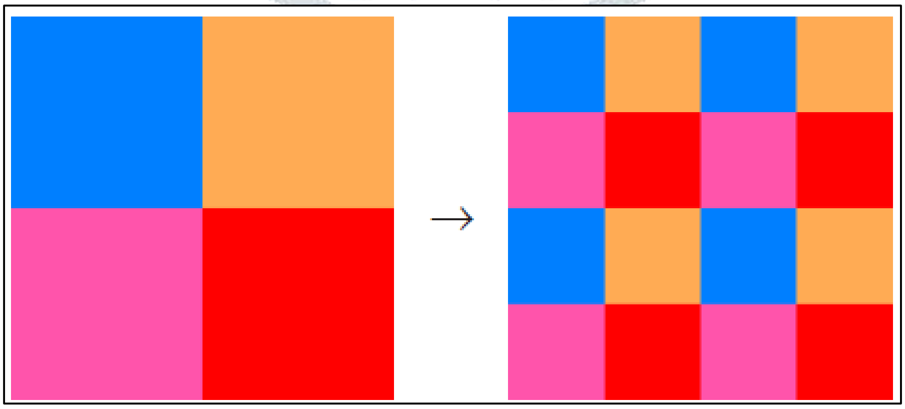


Figure 3: Multi Reduce Permutation of colored image

V. Flowchart of the proposed method

Figure 4 shows the flowchart of the proposed method. This technique can be tested using [30-32].

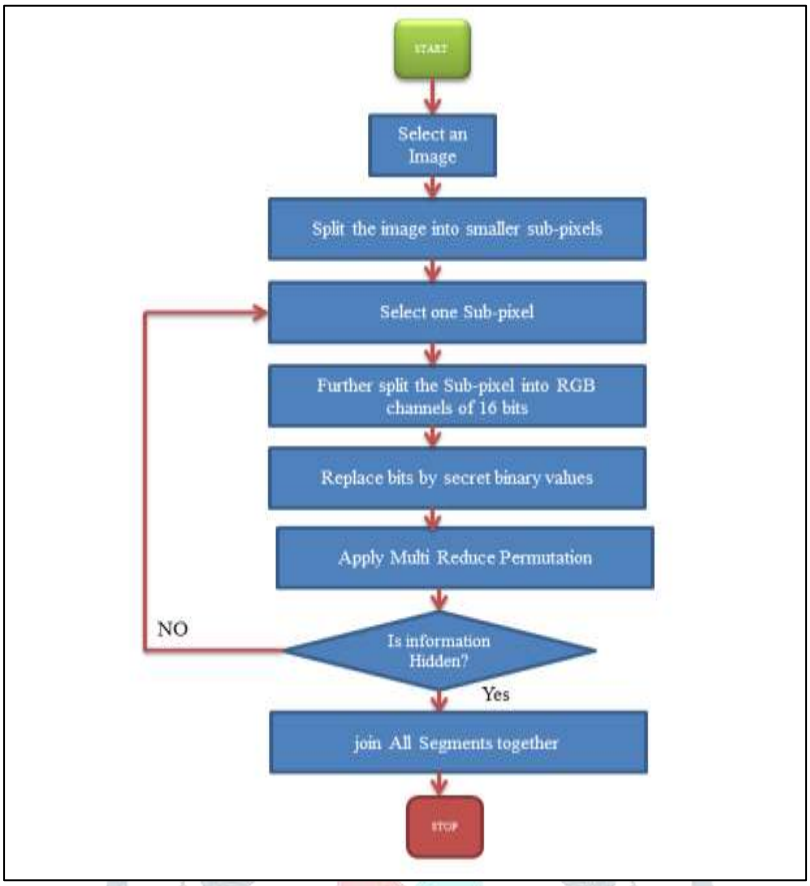

START
Select an Image
Split the image into smaller sub-pixels
Select one Sub-pixel
Further split the Sub-pixel into RGB channels of 16 bits
Replace bits by secret binary values
Apply Multi Reduce Permutation
Is information Hidden?
NO
Yes
join All Segments together
STOP

Figure 4: Proposed method

VI. Algorithm

6.1 Proposed Image Encryption Method

Algorithm: Image Encryption.
Input: Hided Image.
Output: Encrypted Image.

- ✓ **Step 1:** Select an input source RGB image.
- ✓ **Step 2:** Do Multi reduce permutation of the input Image and divide it into several parts.
- ✓ **Step 3:** Each part is then further encrypted into n shares. This encryption will depend on key used.
- ✓ **Step 4:** From Step 3, we get n X n shares.
- ✓ **Step 5:** Apply encryption key.
- ✓ **Step 6:** Select k out of n shares.

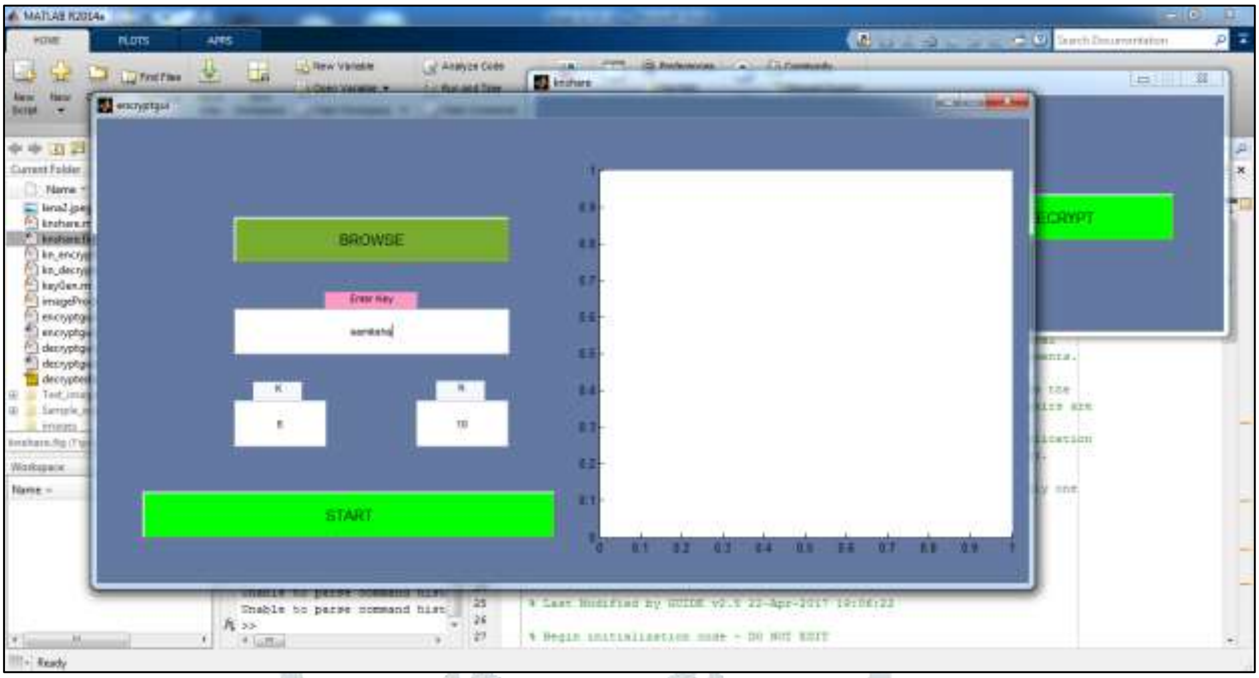
6.2 Proposed Image Decryption Method

Algorithm: Image Decryption.
Input: Final Encrypted Image.
Output: Decrypted Image.

- ✓ **Step 1:** Select an Encrypted RGB Image.
- ✓ **Step 2:** Reverse Multi Reduce Permutation.
- ✓ **Step 3:** Apply same key as for encryption.
- ✓ **Step 4:** Create n shares from each sub part.
- ✓ **Step 5:** From n shares each of step 4, Create (n-1).
- ✓ **Step 6:** Compress Images obtained from step 5 into Decrypted Image.

VII. Results and Analysis

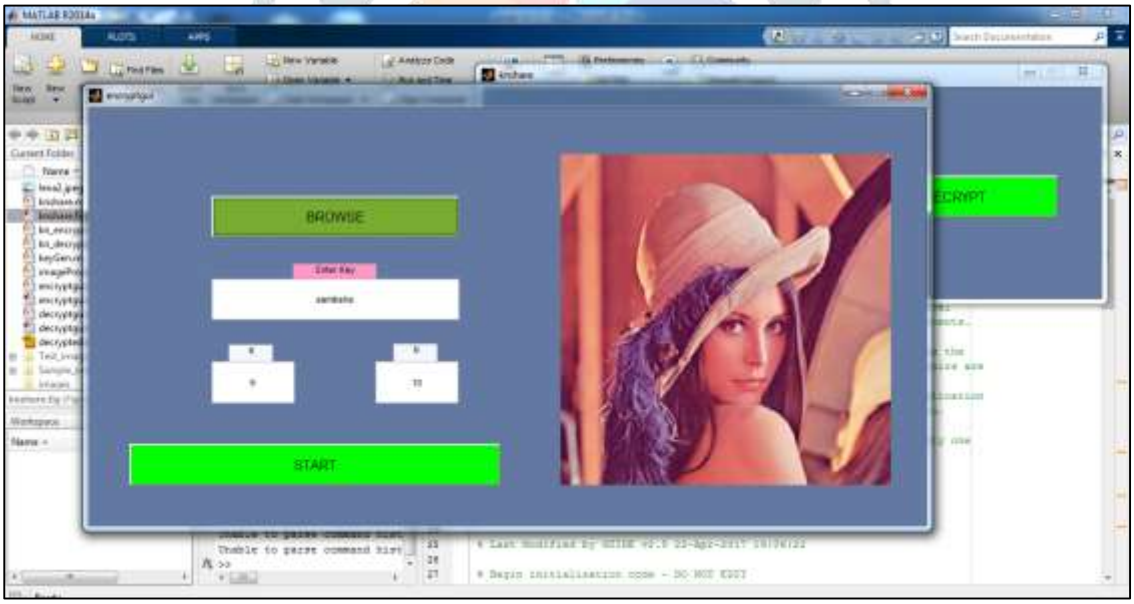
First of all select an image for the encryption. Enter the encryption key, multi reduce permutation value and number of shares as shown in **Fig 5**.



```
Unable to parse command hist
>>
% Last Modified by GUIDE v2.5 22-Apr-2017 19:06:22
% Begin initialization code - DO NOT EDIT
```

Figure 5: Permutation value; value of k; value of n

Select an image as shown in Figure 6. The encrypted image is shown in Fig. 7. Then shares are selected for the image (shown in Figure 8) and the same key is applied for decryption and the image is decrypted successfully as shown in **Fig. 9**.



```
Unable to parse command hist
>>
% Last Modified by GUIDE v2.5 22-Apr-2017 19:06:22
% Begin initialization code - DO NOT EDIT
```

Figure 6: Input Image

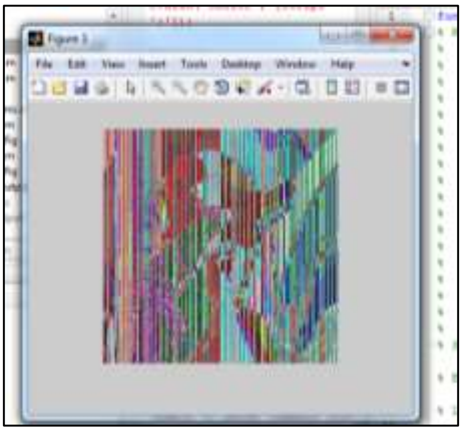


Figure 7: Encrypted Image

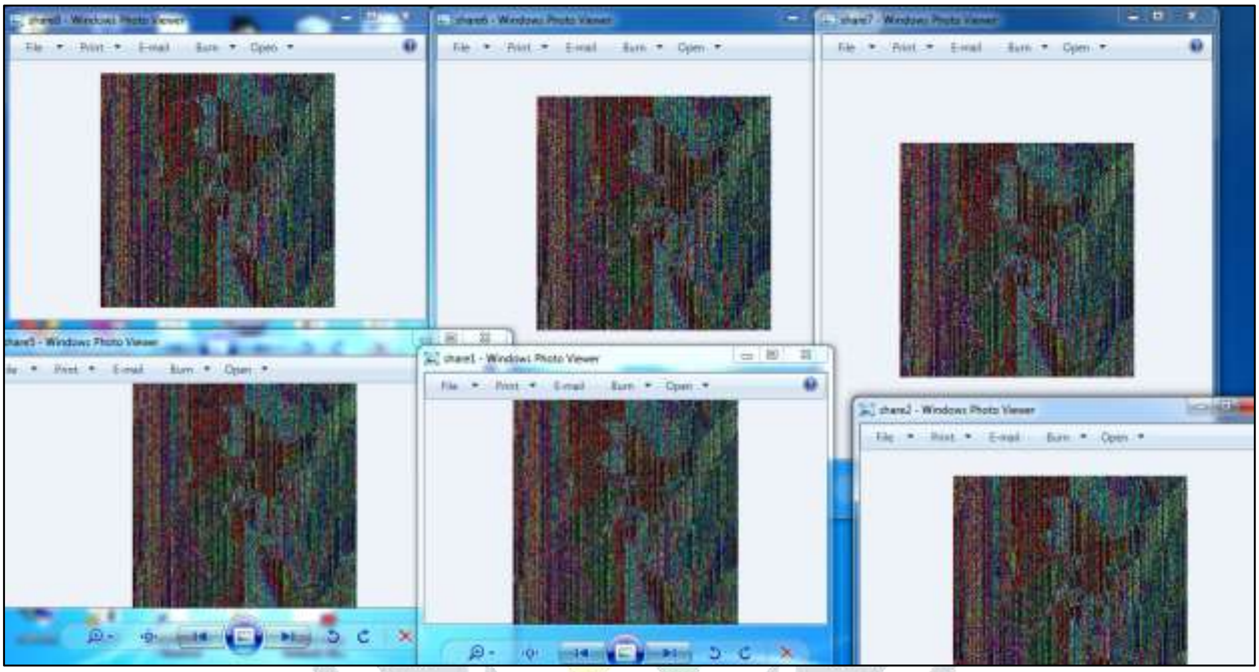

share8 - Windows Photo Viewer
share6 - Windows Photo Viewer
share7 - Windows Photo Viewer
share5 - Windows Photo Viewer
share1 - Windows Photo Viewer
share2 - Windows Photo Viewer
File Print E-mail Burn Open

Figure 8: Shares (n) for the Image.

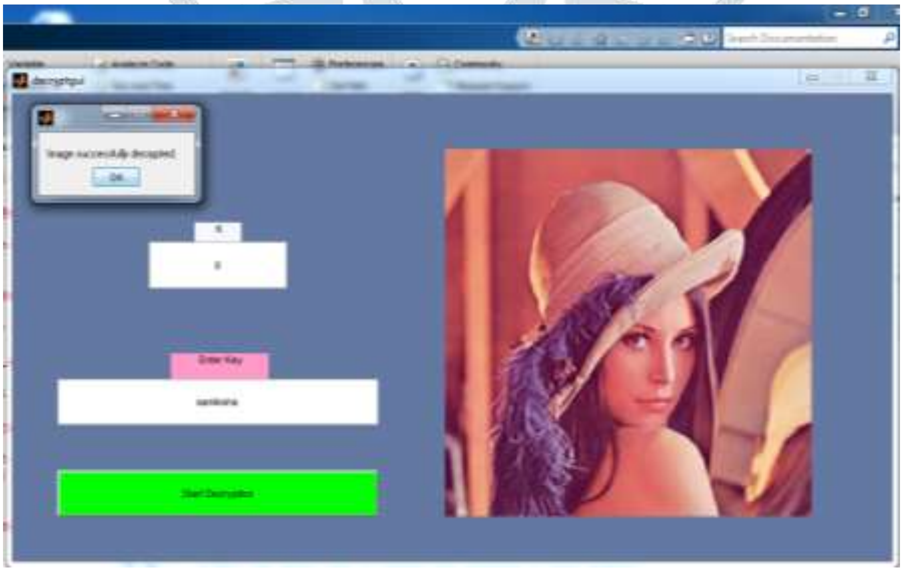


Image successfully decrypted

Figure 9: Image Decryption Successfully

VIII. Conclusion

This work implements a simple visual cryptography for colored images with the method of Multi reduced permuted k out of n shares. This scheme is fast and more secure than previous methods. There is always a room for improvements in any software package, however good and efficient it may be done. But the most important thing should be flexible to accept further modification. Right now we are just dealing with color image encryption and decryption. In future this software may be extended to include features such as: Improved security using HMM model and using Bayesian Theorem.

REFERENCES

[1] Naor, M. and A. Shamir.1995. Visual cryptography, Advances in cryptology. In Proc. of Eurocrypt LNCS, 1–12.

[2] Samiksha, Bhatia, K., Sharma, R. 2018. Cryptographic Techniques: in New Era. International Journal of Advanced Computational Engineering and Networking, 6(3): 49-52.

[3] Sharma, R. 2018. Security Attacks and Prevention in Wireless Sensor Networks. International Journal of Emerging Technology and Advanced, 8(4): 142-148.

[4] Sharma, R. 2018. Jamming Threat to Wireless Sensor Network. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(4): 546-549.

[5] N., Nithin , Bongale, A.M. , Hedge, G. P. 2013. Image Encryption based on FEAL algorithm. International Journal of Advances in Computer Science and Technology, 2(3): 14- 20.

[6] Dutta, M.K. and Nath, A. 2014. Scope and Challenges in Visual Cryptography. International Journal of Innovative Research in Advanced Engineering, 1(11): 38-46.

[7] Priya, G.M. and Kumari, P.V. 2012. Compression of Quasi-Group Encrypted Grayscale Images. International Journal of Scientific and Research Publications, 2(7), 1-4.

[8] Kumar, S.S. and Mangalam, H. 2012. Wavelet-based Image Compression of Quasi Encrypted Grayscale Images. International Journal of Computer Applications, 45(12):35-39.

[9] Ye, R. 2011. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. In Proc. Of Optics Communications, 284(22): 5290-5298.

[10] Al-Maadeed, S., Al-Ali, A. and Abdalla ,T. 2012. A New Chaos-Based Image-Encryption and Compression Algorithm. Journal of Electrical and Computer Engineering, 2012: 1-11.

[11] Bhatt, V. and Chandel, G. S. 2012. Implementation of new advance image encryption algorithm to enhance security of multimedia component. International Journal of Advanced Technology & Engineering Research, 2(4): 17-20.

[12] Dey, S. 2012. SD-EI: A Cryptographic Technique To Encrypt Images. In Proc. Of IEEE international conference in Cyber Security, Cyber Warfare and Digital Forensic, 28-32.

[13] Sharma, R. 2018. Face recognition using principal component analysis: A survey. Proceedings of ARSSS International Conference, 29th April, 2018, Bengaluru, India, 59-62.

[14] Sanju, Bhatia, K. and Sharma R. 2018. An analytical survey on face recognition systems. International Journal of Industrial Electronics and Electrical Engineering, 6(3): 61-68.

[15] Sharma, R. and Lobiyal, D.K. 2018. Intelligent Water Drop Based Coverage- Connectivity and Lifespan Maximization Protocol for Wireless Sensor Networks. Recent Patents on Computer Science, In Press.

[16] Chhillar, P., Bhatia, K. and Sharma, R. 2016. Spiral Based Sink Mobility Method Aiming Lengthening of Lifetime of Sensor Networks. International Research Journal of Engineering and Technology, 3(5): 631-637.

[17] Chhillar, P., Bhatia, K. and Sharma, R. 2016. Swarm Intelligence Inspired Energy Efficient Routing Protocols for Sensor Networks: An Investigation. International Research Journal of Engineering and Technology, 3(5): 623-630.

[18] Hooda, S. Bhatia, K. and Sharma, R. 2016. Enrichment of Life span of Sensor Networks through BCO and Gateway Node. International Journal of Research in Information Technology,4(5): 9-20.

[19] Hooda, S. Bhatia, K. and Sharma, R. 2016. Nodes Deployment Strategies for Sensor Networks: An Investigation. International Research Journal of Engineering and Technology, 3(4): 2499- 2500.

[20] Sharma, R. and Lobiyal, D.K. 2015. Dual Transmission Power and Ant Colony Optimization Based Lifespan Maximization Protocol for Sensor Networks. International Journal of Business Data Communications and Networking, 11(1): 1-14.

[21] Sharma, R. and Lobiyal, D.K. 2015. Region Based Energy Balanced Inter-cluster communication Protocol for Sensor networks. NCCCIP Conference Proceedings, Nirjuli India,184-195.

[22] Sharma, R. and Lobiyal, D.K. 2015. Energy Based Proficiency Analysis of Ad-hoc Routing Protocols in Wireless Sensor Networks. IEEE, Conference Proceedings ICACEA, Ghaziabad, India, 882-886.

[23] Sharma, R. and Lobiyal, D.K. 2015. Proficiency Analysis of AODV, DSR and TORA Ad-hoc Routing Protocols for Energy Holes Problem in Wireless Sensor Networks. Elsevier, Procedia Computer Science, 57: 1057-1066.

[24] Rana, A., Bhatia, K. and Sharma R. 2017. IIEPDR: Improved Information and Energy Proficient Data Relaying Routing Protocol for Wireless Body Area Networks. International Research Journal of Science Engineering and Technology, 7(2): 4-11.

[25] Rana, A., Bhatia, K. and Sharma R. 2017. ETM: A survey on Energy, Thermal and Mobility Efficient Routing Protocols for Wireless Body Area Sensor Network. International Research Journal of Commerce, Arts and Science, 8(4): 26-38.

[26] Sharma, R. 2015. Energy Holes Avoiding Techniques in Sensor Networks: A survey. International Journal of Engineering Trends and Technology, 20(4): 204-208.

[27] Sharma, R. and Lobiyal, D.K. 2015. Multi-Gateway-Based Energy Holes Avoidance Routing Protocol for WSN. Informatics, 3(2): 1-26.

[28] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm.

[29] https://www2.cs.arizona.edu/patterns/weaving/webdocs/gre_iper.pdf

[30] Devi, J. Bhatia, K. and Sharma, R. 2017. A Relative Analysis of Programmed Web Testing Tools. International Research Journal of Engineering and Technology, 4(5): 386-389.

[31] Devi, J. Bhatia, K. and Sharma, R. 2017. A Study on Functioning of Selenium Automation Testing Structure. International Journal of Advanced Research in Computer Science and Software Engineering, 7(5): 855-862.

[32] Sharma, P., Sachdeva, R. and Sharma, R. 2018. Location based Tracking: The need of the hour. International Journal of Engineering Science Invention, 7(5): 50-53.