IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 14, Issue 2, Ser. I (Mar.-Apr. 2019), PP 37-43
www.iosrjournals.org

Database Security Using Multi-Shares Visual Cryptography

Dr. G.D.Dalvi[1], Dr. Mrs.S. D. Wakde[2], Prof. P.V.Kale[3]
[1]*Assistant Professor, P. R. Pote Patil College of Engineering and Management Amravati, (MS) India.*
2Principal,P. R. Pote Patil College of Engineering and Management.Amravati, (MS)India
[3]*Assistant Professor, P.R .Pote Patil College of Engineering and Management Amravati, (MS) India.*
Corresponding Author: Dr. G.D.Dalvi

Abstract: *Security is a basic need of today's digital world. The Concept stated in this paper describes utility of Visible Cryptography (VC) to the authentication of facial pictures. In proposed system, photograph of character is taken care of, once entered it is encrypted and decrypted using sterilization set of policies. In this work useful bitwise operation is performed on every pixel with the help of key which is provided by new concept of sterilization algorithm. Initially it is necessary to separate the R, G and B channel from the image and which will be encrypted on Multiple shares and later to convert the image in such way that original image form only when shares are combined in proper sequence. In current innovation, the greater part of VC is implanted as a mystery utilizing various shares.*

Keywords: *Bitwise operation; Multi shares; Pixel-Sharing; Sterilization Algorithm.*

Date of Submission: 27-03-2019 Date of acceptance: 11-04-2019

I. Introduction

Hiding of Visual data is a critical part over the globe .It is essential to protect the data from unauthorized users. For this purpose researcher have proposed several methods such as Biometrics method which includes Fingerprint, gesture. These security systems are widely used for identification of employees at the entrance of the Organization, banking sectors etc. Principal research issues with these system is to provide the key method for the sequence hence system will look like critical but easy for the encryption and decryption by using sterilization algorithm .The concept of sterilization algorithm is based on VC.

Naor and Shamir proposed a "(k, n)-threshold visible mystery sharing scheme"1994,which is referred as Visible Cryptography [1].The important feature in this system is that the name of a game picture may be decrypted genuinely through the human visible device. Thus there may be no need of the knowledge of VC by the user. Every share looks like collection of Random Pixel and look like a meaningless by itself. The generated share does not provide any information regarding the Original Image [2]. In this research Cryptography can be provided for any format of color image. The mystery key is provided and later sends it to the beneficiary. The collector unscrambles (change over figure content into plain content) the message to get the mystery data. Like cryptography, VC is a procedure which encodes the picture and changes over it into muddled arrangement and by unscrambling the picture unique mystery picture is acquired. Encryption is the way toward changing the picture into some other picture utilizing a calculation so that any unapproved individual cannot remember it. VC is reached out up to mystery sharing [3]-.

Visual mystery sharing scramble a mystery picture into straight forward parts which are called as shares. These shares with the end goal that stacking an adequate number of shares uncovers the mystery image [5]. It is an acquire from mystery sharing plan given by Adi Shamir in 1979 where they have demonstrated to partition information Gas parts r that G is effectively assemble from any C pieces, however even entire learning of c – 1 pieces uncovers definitely no data about information G[6].

VC can likewise be fairly misleading to the unpracticed eye, in a manner that, if a picture share were to fall into the people hands, it would resemble a picture of arbitrary commotion or awful workmanship. Shading VC is the novel approach in which shading picture change over to incoherent arrangement. RGB and its subset CMY shape the most fundamental and surely understood shading model Subtractive hues are apparent if shades in a catechism digest assertive wavelengths of white ablaze while apery the rest. Any brave question, whether accepted or man-made, ingests a few wavelengths of ablaze and reflects or transmits others; the wavelengths larboard in the reflected/transmitted ablaze accomplish up the concealment that can be seen. Red, green and dejected are the capital jolts for animal concealment acceptance and are the capital added actuality hues. The abetting shades of RGB, cyan, maroon, and yellow, are affected by the alloy of two of the primaries and the abstention of the third. Red and blooming consolidate to accomplish yellow, blooming and dejected accomplish cyan, dejected and red accomplish fuchsia. White ablaze is fabricated if all shades of the EM ambit accompany in abounding force..

Rest of the paper is organized as follows: section2 summarizes related works on this topic. Section 3 discuses the overview of proposed work. Section 4 is describing the proposed methodology with various data flow and charts. Section 5 finally concludes the work.

II. Related Work

Cryptography modified into in the beginning invented and pioneered with the useful resource of Naor and Shamir [7] in 1994 on the Eurocrypt convention. The (adequate, n) visible Cryptography Scheme can decode the concealed snap shots with none cryptographic computations. It consists of black and white pixel only and it was for sharing single thriller. the decision of the sport photograph is break up into precisely random stocks i.e. Share1 and Share2. To expose the original picture, every shares are required to be stacked. Whilst stocks are superimposed, if white pixels overlap, the ensuing pixel may be white and if a black pixel in one percentage overlaps with both a white or black pixel in a few special percent, the ensuing pixel may be black. which means that the superimposition of the shares represents the Boolean OR function.

Extended visible cryptography changed into proposed currently to construct meaningful binary snap shots as shares. The use of hyper graph colors, however the visual fine is poor to triumph over this problem in 2006, Zhou et.al. [9] recommended a singular approach named halftone visual cryptography to gain visible cryptography via half firming. It simulates continuous tone imagery via the use of dots, which can also range either in length, in form or in spacing. This method makes a specialty of growing a standard halftone VC framework, wherein a secret binary photo is encrypted into first-rate halftone pictures, or halftone stocks. The proposed method applies the rich concept of blue noise half of firming to the development mechanism utilized in conventional VC to generate halftone shares, even as the security residences are still maintained. The proposed technique utilizes the void and cluster set of rules to encode a secret binary image into n halftone stocks wearing substantial visual information. The visible first-rate of acquired halftone shares is observably higher than any available VC technique recognized to this point. It maintains suitable evaluation and security and increases best of the stocks.

Simple Visual Cryptographic technique is insecure. This cryptographic technique involves dividing the secret image into n shares and a certain number of shares (m) are sent over the network. The decryption process involves stacking of the shares to get the secret image. To overcome this problem Sharma and Saraswat in 2013[11] proposed a cryptographic technique for color images where they are using color error diffusion with XOR operation. The shares are developed using Random number. The key generated for decryption process is sent securely over the network using RSA algorithm. Error diffusion is a type of half toning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. If Half Gray is above then white pixel generated and for Below black pixel is generated if full black or full white then error in the image. By adding the error in next pixel process is repeated.

Bhakta, [12] in 2013 proposed a method where they perform encryption at several levels. First they had used a variable length image key to encrypt the original image then bit sieve procedure used on resultant image and lastly they performed k-n secret sharing scheme on the final encrypted image. Decryption is done in reverse level of encryption that means do k-n secret sharing scheme, bit sieve method and image key decryption respectively. As multiple levels of encryptions are being used the security is increased manifold.

This technique of well known image key based encryption, key based bit sieved encryption and k-n secret sharing based encryption as they used multiple level of encryption thus the security is increased. As image key and bit sieve based key are known in between sender and receiver, the security is increased. They had split specific k numbers of shares among n number of shares thus provide a more secured system. Mathematical calculation compared with other existing techniques of secret sharing on color images is very much less.The computation speed is increased. However in this technique they had send huge additional information for image key based encryption, key based bit sieved encryption and k-n secret sharing scheme which need more memory.

Haque,. Rahul [13] proposed a way of visible cryptography for colored pictures in 2013.They used RGB color model for color pictures to begin with, photograph is break up into monochromatic channels then converts every person image to binary photo. Later they compiled with easy VCS scheme. The decision of game picture may be recovered through manner of stacking proportion pictures. Every pixel is of a 32 bit. Sample pixel is represented in the following determine:-A 32 bit sample pixel is represented in the following figure:-

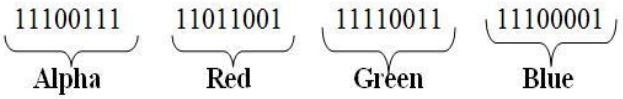

Fig. 1- Separation of Alpha, Red Green and Blue Channel

Virtual shade picture are divided into 4 components, Alpha, Red, Green and Blue; each with 8 bits. Alpha thing represents degree of transparency. If all bits of Alpha element are 'zero', then the photograph is absolutely obvious. The usage of color errors diffusion approach improves the first-class of encrypted image. The XOR operation is applied in stacking to produce the better photograph and there can be no growth inside the length of decrypted photograph. The primary (adequate, n) threshold VCS is used for coloration photos wherein the size of proportion photographs is nk-1. The gadget has become in particular relaxed.

In 2014 Shubhra [14] proposed a technique for (2, 2) seen cryptography and (three, three) seen mystery sharing. They proposed mystery sharing using randomized VSS in which new seen cryptography algorithm for gray scale picture the use of randomization and pixel reversal approach is given. (2, 2) Randomize visible cryptography, wherein the stocks are generated primarily based on pixel reversal, random bargain in unique pixel and subtractions of the particular pixel with previous shares pixel. The proper mystery photograph is cut up on this form of manner that once OR operation of certified stocks exhibits the call of the game photograph inside the (3,3) visible thriller sharing scheme, shares are generated based mostly on pixel reversal, random discount in genuine pixel and subtractions of the unique pixel with previous stocks pixel and storing the final fee of the share pixel after reversal into the stocks in round robin fashion. The end result of the 3 shares obtained after OR operation using stacking of a whole lot of those licensed shares, the premaster display.

In 2015 Shankar K and Eswaran P [15], they proposed visual cryptography method is utilized to send a unique picture from the sender to the recipient with preeminent classification and mystery. From the mystery picture the RGB shading band of the pixel qualities are taken and make the different grid (Ri, Gi, Bi) [13]. The essential frameworks R1, R2, G1,G2 and B1,B2 are acquired by isolating every single an incentive in Ri, Gi and Bi by 2. Create globalized key network arbitrarily (Km , where m=0, 1, 2...255) in view of size of the fundamental frameworks. At that point, the XOR(Km, R1) and XOR(Km ,R2) plays out a XOR work on the components of R1 and R2 lattices with key framework Km independently and get the resultant networks as RS1 and RS2 in Ri grid. This procedure is rehashed for making GS1, GS2 and BS1, BS2 in Gi and Bi networks also. In this procedure, shares and AES calculation ties together to give the resultant shares are known as the epitomized offers It is utilized to secure the shares from enemies or aggressors. The whole proposed encryption forms depicted.

In 2016 Linju P.S and Sophia Mathews [16] proposed framework, two mystery shading pictures are utilized which can be isolated into three partakes altogether. At first, these mystery pictures ought to be changed into its halftone representations. At that point enhanced preprocessing stage employments the basic piece substitution strategy and the halftone pictures are preprocessed utilizing SBR procedure. Henceforth these are changed over into preprocessed pictures. Since the pictures are shading pictures, both preprocessing and also half toning must be performed in 3 planes R, G and B. Once these procedures are finished, 3 shares are created. At this organize, the framework ask for 3 cover pictures. These solicitations are met by shareholders by giving the cover pictures and subsequently inserted cover picture share is gotten. The shares gotten are superimposed by utilizing a specific approach to get the last mystery picture. This yield overcomes the normal confinements like loss of picture clarity and in addition pixel extension. Alongside this, the framework likewise gives a tricking aversion system which can forestalls both tricking between share members and duping to the picture content proprietor.

III. Proposed Work

The result of the proposed work may have a few application in the field of picture processing, Secure confirmation and will affect security applications. Proposed technique will help in execution of this examination for picture preparing application.

- Authentication will be more secure in constant applications.
- Proposed Sterilization calculation is used as devoted framework equipment.
- Proposed framework will help in security application outlining.
- Low PSNR and high MSE for Encrypted picture and High PSNR and low MSE for unscrambled picture can be useful for precision.

IV. Proposed Methodology

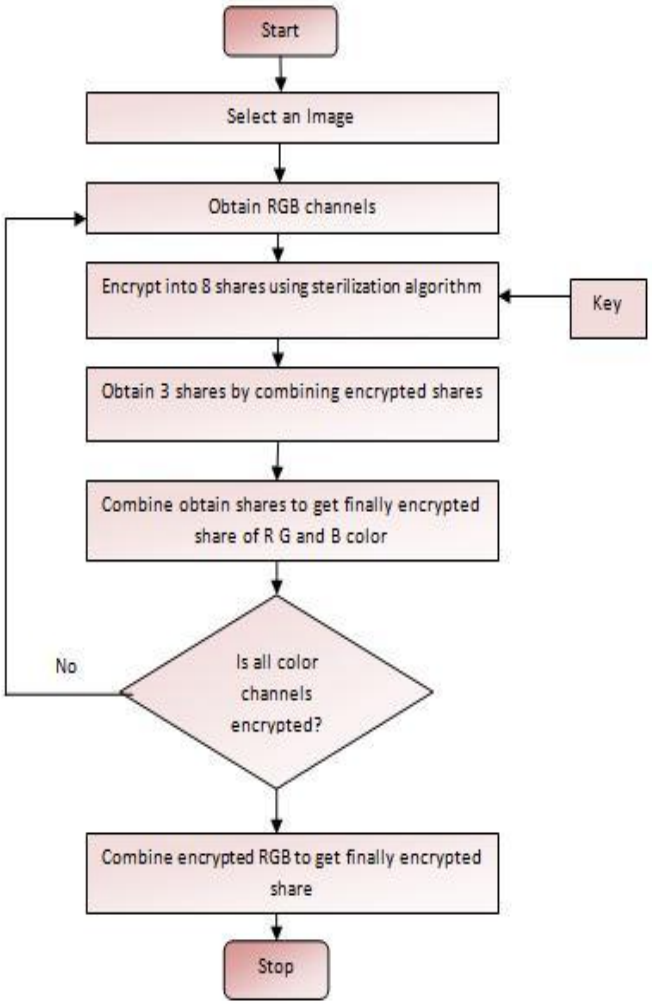

Fig. 2-Flow Chart of Design Process

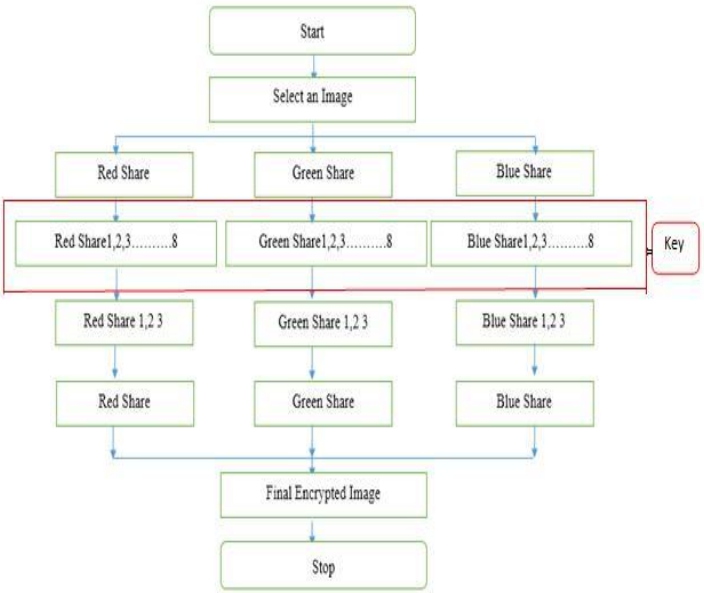

Fig. 3-Data Flow diagram For Encryption

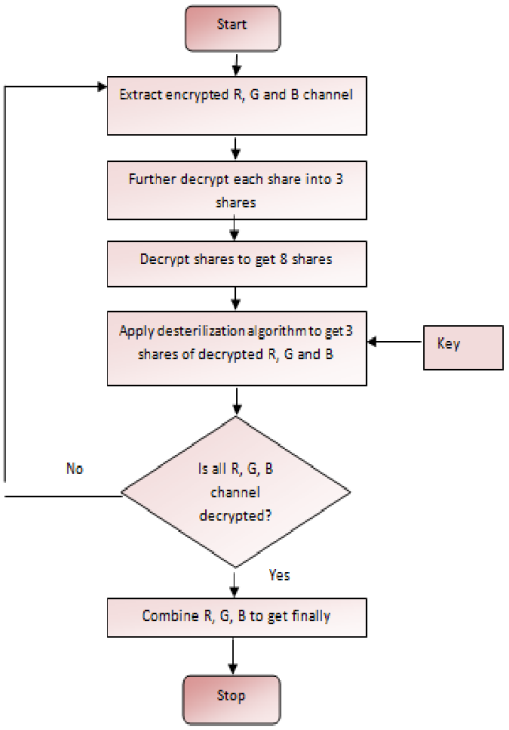

Fig. 4-Flow Chart for Decryption of image.

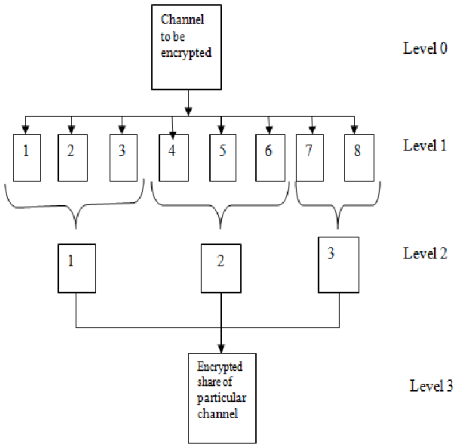

Fig. 5-Encryption of Channel

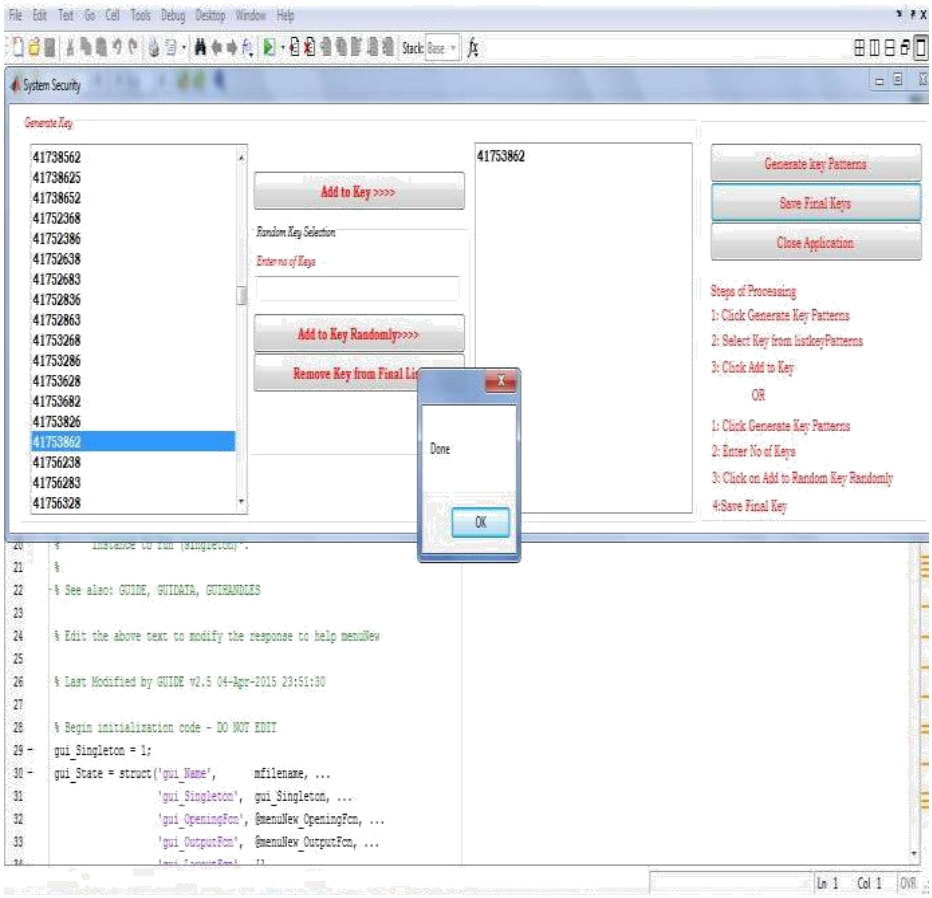

Fig. 6-Generation of Key Pattern

Fig 2 is about the design process of proposed research, we first select the image, from this selected image we generate three (R, G, B) channels. Thesegenerated RGB channels are again used to create the eight shares from each channel by using keys with the help of permutation method .In the next level again we generate the three shares by combining the (3,3,2) shares in next level. Later by combing these shares we generate the single Red channel repeating the same procedure for Green and Blue channel and in last level combine Red, Green and Blue channel to generate the Encrypted image. The encryption of image is done through Sterilization algorithm and for decryption the Desterilization Algorithm is used.

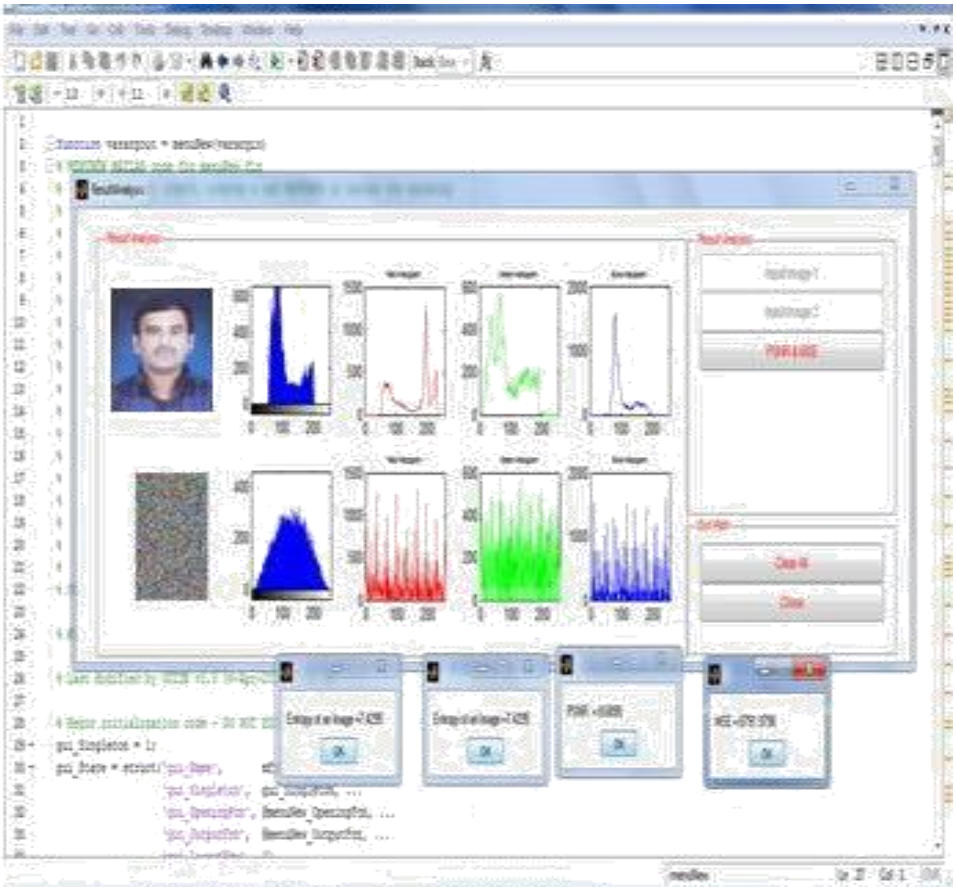

Fig. 7-Display of GUI for Result Analysis

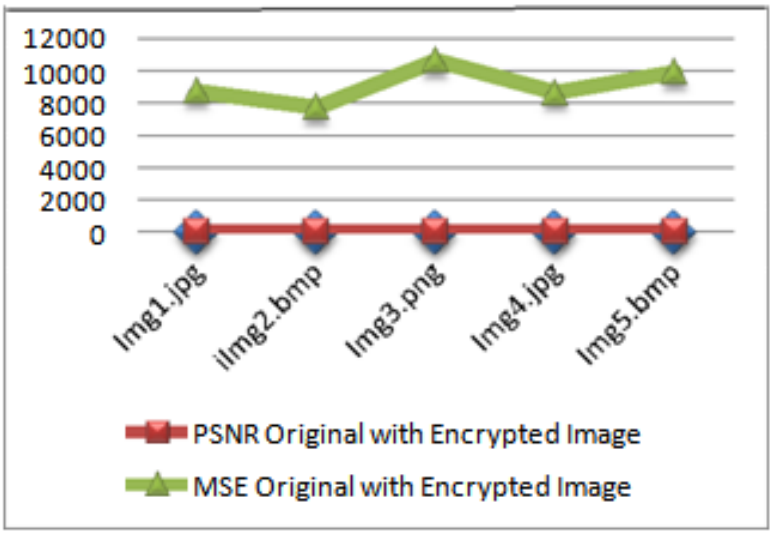

Fig. 8 -Experimental Result Analysis

Table 1- Comparison table

Name of Input Image	**PSNR Original with Encrypted Image**	**MSE Original with Encrypted Image**
Img1.jpg	8.6899	8791.97
Img2.bmp	9.2215	7779.12
Img3.png	7.8407	10690.76
Img4.jpg	8.7402	8690.78
Img5.bmp	8.1558	9942.60

V. Conclusion

This paper proposes a novel idea of facial image authentication using sterilization algorithm in VC. In this work new concept of sharing the color image at multiple levels has given to provide more security to the encryption. Encryptions performed by separating Red, Green and Blue channels and then Sterilization Algorithm is used. It provides keys which are used to encrypt every component of a pixel. Each level consist of database of particular number of shares, by using that database image is encrypted or decrypted. For revealing the original image all the shares are required to be superimposed using the keys. By stacking shares in proper sequence original image will be obtained. The concept is extremely secure as shares are encrypted at multiple levels using the keys without which one can never decrypt the image In future, proposed method can be extended to apply with multi-path routing. Its focus will be delay, energy efficiency and packet delivery ratio.

ACKNOWLEDGMENT

The authors would like to thank S.V. Dudul and other staff members of SGBAU for their valuable help.

References

[1]. M. Naor and A. Shamir, "Visual cryptography," Advances in Cry ptology - EUROCRYPT'94, Springer-Verlag,1995,Vol-950, pp.1-12.
[2]. Hsien-Chu Wu ,Hao-Cheng Wang and Rui-Wen Yu“ Color Visual Cryptography Scheme Using Meaningful Shares, ” ISDA’ 08,Vol ,3;pp 173-178,Nov,2008.
[3]. J. K. Mandal and Subhankar Ghatak, “Constant Aspect Ratio based (2, Visual Cryptography through Meaningful Shares (CARVCMS)”. IEEE 1ST International conference on communication and Industrial application (ICCIA-2011 Paper ID 92), December 2011, pp.01-04.
[4]. Meera Kamath, Arpita Parab, “Extended Visual Cryptography for Color Images Using Coding Tables”, 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, India 978-1-4577-2078-9/12 2011 IEEE.Vol4,Issue 5,Oct-2011,pp 39-46.
[5]. Yanyan Han and Haocong Dong, “A Verifiable Visual Cryptography Scheme Based on XOR Algorithm”, 978-1-4673-2101-3/12/$31.00 2012IEEE.
[6]. Kulvinder Kaur and Vineeta Khemchandani “Securing Visual Cryptographic Shares using Public Key Encryption”, 978-1-4673-4529-3/12 IEEE.
[7]. Naor, M. and Shamir, A., “Visual cryptography, “In Proc. Eurocrypt 94, Perugia, Italy, Springer Verlag, May 912, LNCS 950, pp. 112.,2010.
[8]. Giuseppe Ateniese, Carlo Blundo and Alfredo De Santis, “Visual Cryptography for General Access Structures”, information and computation 129, 86106 (1996), article no. 0076 0890-5401_96 _18, 1996.
[9]. Z. Zhou, G. R Arce, and G. Di Crescenzo, “Halftone Visual Cryptography,” in Proc. of IEEE International Conference on Image Processing,Barcelona, Spain, VOL. 15, NO. 8, August 2006 .
[10]. S. J. Shyu,S. Y. Huang, Y.K. Lee, R.Z.Wang, Kun Chen, “Sharing multiple secrets in visual cryptography,” Elsevier Ltd doi:10.1016/j.patcog.03.012-0031-3203/$30.00-2007.
[11]. Manika Sharma, Rekha Saraswat, ” Secure Visual Cryptography Technique for Color Images Using RSA Algorithm”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013
[12]. Anupam Bhakta, Sandip Maity, Ramkrishna Das, Saurabh Dutta,” An Approach of Visual Cryptography Scheme by Cumulative Image Encryption Technique Using Image-keyEncryption,Bit-Sieved Operation and K-N Secret Sharing Scheme,” International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-1, June 2013.
[13]. Mohd. Junedul Haque, Mohd. Muntjir, Mohd. Rahul,” Image Encryption An Intelligent Approach of Color Visual Cryptography” International Journal of Computer Applications (0975 – 8887) Volume 83 – No 5, pp.7-9 December 2013.
[14]. Shubhra Dixit,Deepak Kumar Jain, and Ankita Saxena, “An Approach for Secret Sharing Using Randomised Visual Secret Sharing," IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies ,978-1-4799-3070-8/14 $31.00 ,2014.
[15]. Shankar K, Eswaran P "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography” Sciencedirect, 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS, 70 (2015) 462 – 468,2015.
[16]. Linju P.S, Sophiya Mathews “ An Efficient Interception Mechanism Against Cheating In Visual Cryptography With Non Pixel Expansion Of Images” International Journal of Scientific & technology Research Volume 5, issue 01, 102-106,January 2016 .