International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 299-303 Jan 2019-June 2019 www.csjournals.com

Visual Cryptography for Color Images Using Sterilization Algorithm

Dr.G.D.Dalvi
Assistant Professor
P.R.Pote Patil College of Engineering and Management
Amravati(MS)

Dr.Mrs. S.D.Wakde
Principal
P.R.Pote Patil College of Engineering and Management
Amravati(MS)

Prof. P.V.Kale
Assistant Professor
P.R.Pote Patil College of Engineering and Management
Amravati(MS)

Abstract: The Concept stated in this paper describes utility of Visible Cryptography (VC) to the authentication of facial pictures. Today's most important issue is security for the images and videos. VC is a technique in which secret image is converted in unreadable format in the encryption and original image is obtained by the decryption process .Particular algorithm is used for encryption and decryption in VC any unauthorized person cannot recognize it. Important functional requirement of VC scheme is to maintain the size of secret image which should be same as original image to avoid the doubt of unauthorized user.

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

I.INTRODUCTION

Covering up of Visual information is a basic part over the globe .It is basic to shield the information from unapproved clients. For this purpose researcher have proposed several methods such as Biometrics method which includes Fingerprint, gesture. These security frameworks are broadly utilized for ID of representatives at the passageway of the Organization, saving money segments and so on. Principal research issues with this system are 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.

In the initial stages of work on secret sharing Moni Naor and Shamir [1] considered only scheme with a(k,n)-threshold access structure. Anyone who holds fewer than n-shares cannot find the any information about the original image. When the n-shares overlap formed the secret image and it can recognized directly by the human visual system. Secret image may be text, pictures, handwritten documents .Wang and Hsu proposed a tagged VC (TVC) scheme in which TVC is capable of hiding tag images in to randomly selected shares however the coding process of TVC and multi-secret scheme bring direction to shares, which definitely lowers the visual quality of the decoded secret image. Extended TVC is called the lossless TVC (LTVC) these scheme encodes the tag images without affecting the rebuild secret images[2].

All the aforementioned studies focus on secret images due to the flexibility in practical applications and complexity in theoretical interest the sharing of multiple secret images, in which different combinations of shares reconstruct different secrets become a significant research topic. The related studies in the literature can be classified in to two categories in terms of decoding process 1) Direct Superimposition only where the shares are stacked directly on to each other .2) Allowing additional operation before superimposition ,where at least one of the shares is allow to one or more operation.[3].

In VC encrypted the secret image in to numbers of shares. These are binary images it usually presented in transparencies VC needs no complicated computation for regeneration of secret images .The process of decryption is to simply overlap the shares and view the secret image that appears due to overlapping of the images.VC techniques is mostly used for the transmission of secured data in military, text images, internet voting etc.[4],[10].

Rest of the paper is organized as follows: section2 summarizes related works on this topic. Section 3 discuss 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

Young-Chang Hou [5] have presented a technique for visual cryptography of color images in 2002 which consist of three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology method, and the color decomposition method. His technique gives us backward capability with the old results in black and white VS along with advantages of black and white VS which are very helpful visual system to decrypt secret image without computation like t out of n threshold scheme which can be applied to gray level and colorful images.

Sabu M Thampi[6] have presented an information hiding technique in 2004 in which a brief history of steganography is explained along with techniques that were used to hide secret information , Textual audio and image based information hiding techniques like least significant bit (LSB) insertion technique in which embed the information in graphical image file, masking and filtering techniques in which by making an image in a manner similar to paper watermarks and transformation techniques which is done by using discrete cosine transformation or wavelet transform to hide information in significant areas of image.

In Koo Kang et.al[7] have proposed a new data hiding method in 2009, a color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations error diffusion and pixel synchronization basic principles used in the generation of shares.

Jagdeep Verma et.al.[8] proposed scheme will add the merits of both visual cryptography as well as Invisible and Blind watermarking techniques in 2012,

Pallavi Chavan et.al [9] Idea stated in this paper describes the application of hierarchical visual cryptography to the authentication system. This is an alternative approach for fingerprint based authentication mechanism.

In 2015 Shankar K and Eswaran P [11], these 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].

In 2016 Linju P.S et.al [12] proposed framework and 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.

III. Proposed Work

The main objective of the proposed research work is to provide easy processing image encryption by using bit-wise operation on every pixel. To perform this VC sterilization method is provided by which image is going to encrypted on multiple level and with the help of desterilization algorithm original image is revealed.

Main objectives of these proposed methods are.

- To give serious reconnaissance to a picture at various levels utilizing different shares. To provide higher complexity to every pixel.
- To reduce the time required for overall process of visual encryption and decryption.
- To reduce the time required for overall process of visual encryption and decryption.
- To provide more security for images.
- To provide low computation, complexity, high efficiency and resolution.
- To improve the image quality of reconstruct images.

IV. Proposed Methodology

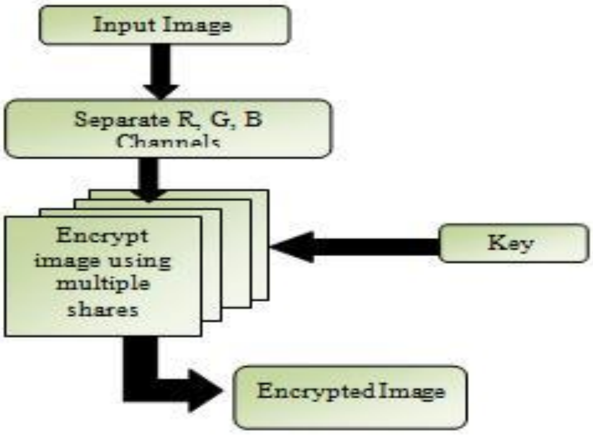

Input Image
Separate R, G, B Channels
Encrypt image using multiple shares
Key
Encrypted Image

Fig. 1-Architecure of Encryption.

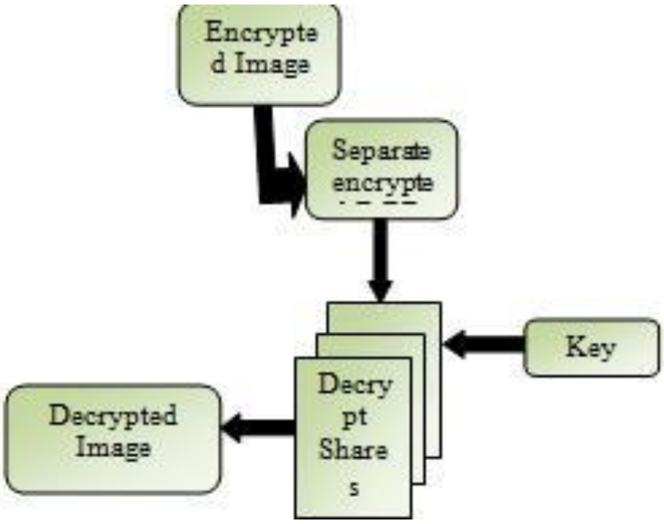


Fig. 2- Architecture of Decryption

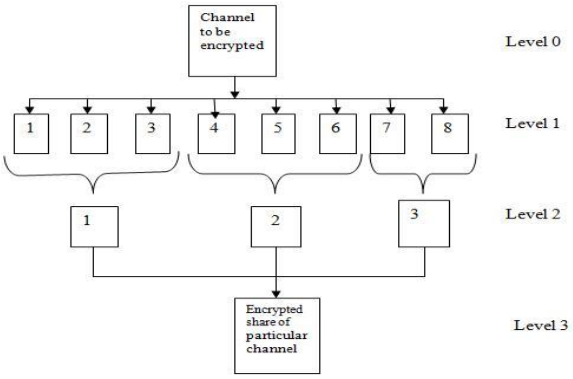


Fig.3-Encryption of Channel

Proposed methodology has been divided into 2 phases.

1) Image Encryption
2) Image Decryption

1. Image Encryption:-

In this image encryption phase, image is encrypted at multiple levels by using multiple shares. It must be color image i.e. red, green and blue component must be present in that image. The image is converted to unreadable format by splitting secret image into forty shadow images or shares. At very first step image is converted into monochromatic one by separating all the three channels i.e. Red, Green and Blue. Then each channel is encrypted into eight shares by using key. These eight shares are further encrypted by making group of shares i.e. First three shares gives first share, next three shares gives second share and remaining two shares gives third share. In these step total 3 encrypted shares are obtained. Combine three encrypted shares from previous step to get encrypted share of each Red, Green and Blue channel. At last level all encrypted shares from previous step need to combine to produce finally encrypted image. At each stage of encryption the database of previous level shares is required.

2. Image Decryption :-

The image decryption method work exactly opposite as that of the image encryption phase. Initially encrypted red, green and blue channels are separated from encrypted secret image. Further each channel produces three decrypted shares by using database from previous stage. At this step nine shares are obtained. Each share from previous step decrypted into further shares to give eight shares. The shares get stored in the database for further decryption. The key is used to decrypt eight shares of each colour to produce originally separated red, green and blue channel. Combine all the three channels to get decrypted image which is similar to that of secret input image. At every stage of decryption it required database of previous step for performing further operation.

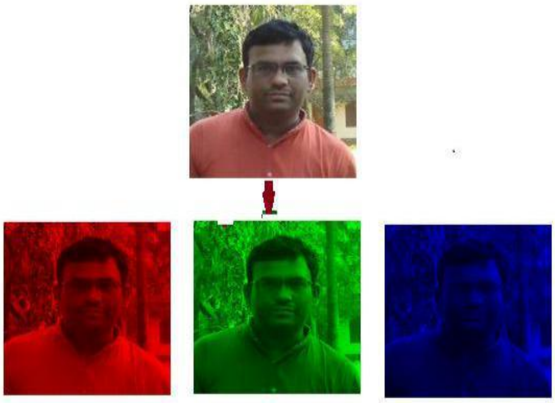


Fig.4-Seperations of R, G,B channels

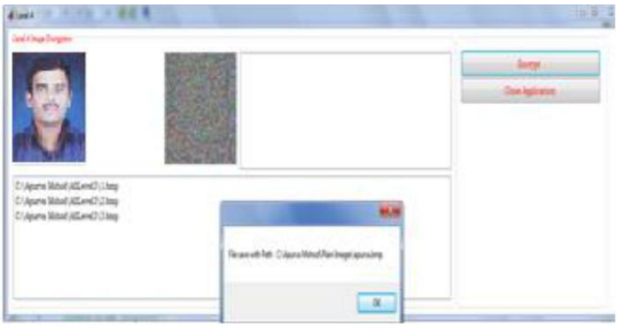
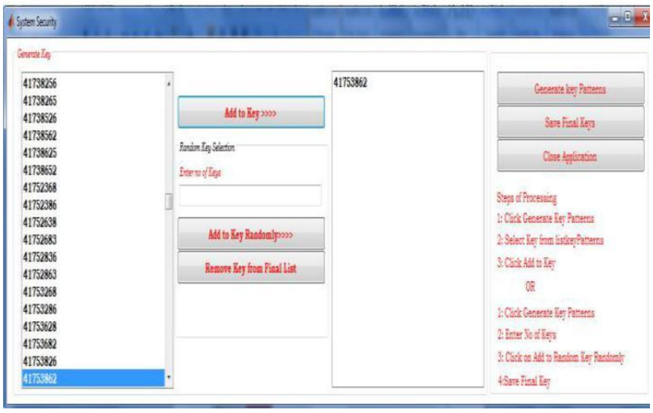


Fig.5- Display GUI for Image Encryption (Level 4)

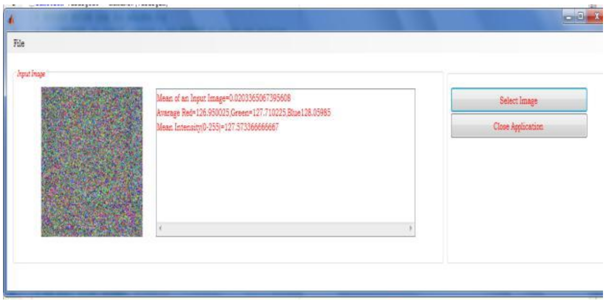


41738256
41738265
41738526
41738562
41738625
41738652
41752368
41752386
41752638
41752683
41752836
41752863
41753268
41753286
41753628
41753682
41753826
41753862

41753862

Steps of Processing
1: Click Generate Key Patterns
2: Select Key from listkeyPatterns
3: Click Add to Key
OR
1: Click Generate Key Patterns
2: Enter No of Keys
3: Click on Add to Random Key Randomly
4:Save Final Key

Fig.6- Display GUI for Selecting Keys



Mean of an Input Image=0.0203365067395608
Avarage Red=126.950025,Green=127.710225,Blue128.05985
Mean Intensity(0-255)=127.573366666667

Fig.7- Display GUI for Image Decryption (Level 4)

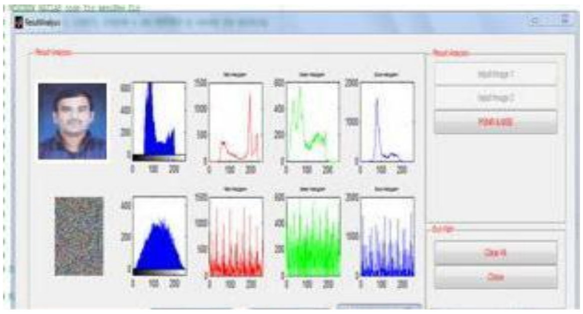


Fig. 7-Display of GUI For Result Analysis

Analysis with respect to PSNR value, MSE and Time Constraint.

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codes. The motion for this situation is the first information, and the commotion is the mistake presented by pressure. When looking at pressure codes, PSNR is estimation to human view of reproduction quality. Despite the fact that a higher PSNR for the most part demonstrates that the reproduction is of higher quality, now and again it may not. One must be amazingly watchful with the scope of legitimacy of this picture; it is just definitively substantial when it is utilized to think about outcomes from the same codec (or codec sort) and same substance. PSNR can be calculated as,

$$\text{PSNR}= 10log_{10}\frac{255^2}{MSE}$$

Where, MSE is the cumulative squared error between the compressed and the original image. The time required for encryption and decryption of an image is also an important factor.

Input Image	M.I Original Image	M.I Encrypted Image	M.I Decrypted Image
Img1.jpg	113.322	127.573	113.322
Img2.bmp	113.453	128.839	113.453
Img3.png	79.509	126.756	79.509
Img4.jpg	127.762	128.228	127.762
Img5.bmp	104.247	122.655	104.247

TABLE. 1- Comparison between Mean Intensity of Original, Encrypted and Decrypted Image

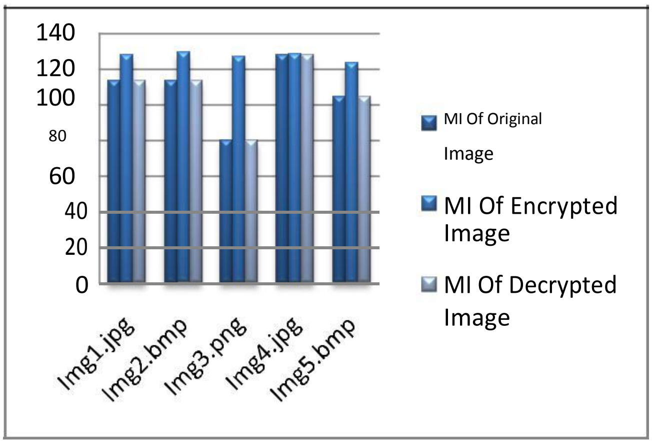


Fig.8- Graph shows relation between Mean Intensity of Original, Encrypted and Decrypted Image

Input Image	Encryption Time (sec)	Decryption Time (sec)
Img1.jpg	1.3554	1.2342
Img2.bmp	1.6854	1.3562
Img3.png	1.7004	1.6385
Img4.jpg	2.0124	1.6678
Img5.bmp	1.6692	1.5232

TABLE. 2- Comparison of Encryption and Decryption time required for level 3.

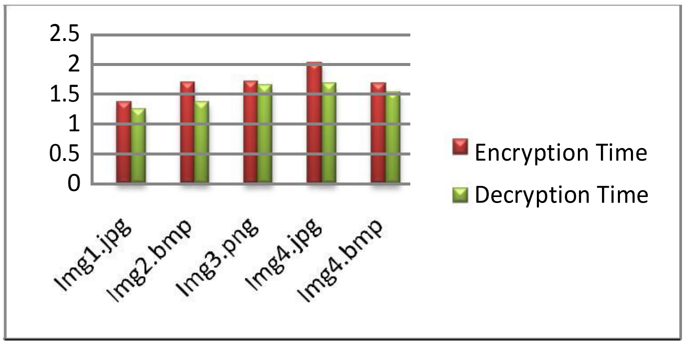


Fig.9- Graph shows relation between Encryption and Decryption time required for Level 3.

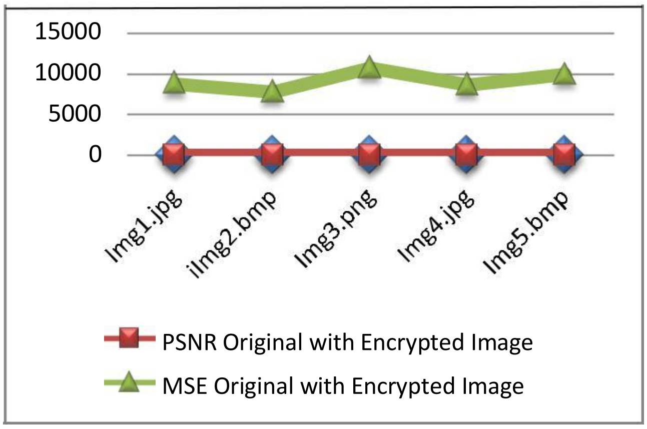


Fig. 8 -Experimental Result Analysis

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 uncovering the first picture every one of the shares are required to be superimposed utilizing 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 Prof.S.G.Fale 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, Vol-950, pp.1-12.Springer-Verlag,1995,

[2] R-Z.Wang and S-F. Hsu, "Tagged Visual Cryptography". IEEE Signal Process.Lett,vol.18,no.11,pp.627-630,2011.

[3] Yanyan Han and Haocong Dong, "A Verifiable Visual Cryptography Scheme Based on XOR Algorithm", 978-1-4673-2101-3/12/$31.00 2012,IEEE.

[4] Kulvinder Kaur and Vineeta Khemchandani "Securing Visual Cryptographic Shares using Public Key Encryption", 978-1-4673-4529-3/12 IEEE.

[5] Young-Chang Hou" Visual cryptography for color images" *Pattern Recognition 36 (2002)* .

[6] Sabu M.Thamp,"Information Hiding Techniques: A Tutorial Review*", ISTE-STTP on Network Security &Cryptography , LBSCE2004.*

[7] InKoo Kang, Gonzalo R. Arce and Heung-Kyu-Lee," color extended visual cryptography using error diffusion", *978-1-4244-2354-5/09/$25.00 ©2009 IEEE.*

[8] Jagdeep Verma, Dr.Vineeta Khemchandani," A Visual Cryptographic Technique to Secure Image Shares", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1,Jan-Feb 2012.

[9] Anuprita U. Mande and Manish N. Tibdewal," Parameter Evaluation and Review of Various Error-Diffusion Half toning algorithms used in Color Visual Cryptography", International Journal of Engineering and Innovative Technology (IJEIT) Volume2,Issue8,February2013.

[10] 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.

[11] Shankar K, Eswaran P "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography" Science direct, 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS,70 (2015) 462 – 468,2015.

[12] 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 .