Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9419-9424, 2017
ISSN: 1816-949X

Extended Visual Cryptography For Color Images Using Sterilization Algorithm

[1]Gopal D. Dalvi and [2]D.G. Wakde
[1]Department of Electronics and Telecommunication,
P.R. Pote Patil College of Engineering and Management,
Amravati University SGBAU, Amravati, India
[2]P.R. Patil College of Engineering and Management,
Amravati, India

Abstract: The concept stated in this study 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.

Key words: Bitwise operation, multi shares, pixel-sharing, sterilization algorithm, functional, unauthorized

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 frame research 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 onVC. In the initial stages of research on secret sharing (Naor and Shamir, 1994) 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 (2011) 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 (Wang and Hsu, 2011).

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 direct superimposition only where the shares are stacked directly on to each other. Allowing additional operation before superimposition where at least one of the shares is allow to one or more operation (Han *et al*., 2012). In VC encrypted the secret image in to numbers of shares. Shares 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. (Kaur and Khemchandani, 2013; Dixit *et al*., 2014).

Literature review: Hou (2003) 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 compability with the old results in black and white VS along with advantages of black and white VS which are very helpful visual system

Corresponding Author: D.G. Wakde, P.R. Patil College of Engineering and Management, Amravati, India

to decrypt secret image without computation like t out of n threshold scheme which can be applied to gray level and colourful images.

Thampi (2008) 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 study water marks and transformation techniques which is done by using discrete cosine transformation or wavelet transform to hide information in significant areas of image.

Kang *et al.* (2011) 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. Verma and Khemchandani (2012) proposed scheme will add the merits of both visual cryptography as well as invisible and blind water marking techniques.

Mande and Tibdewal *et al.* (2013) idea stated in this study describes the application of hierarchical visual cryptography to the authentication system. This is an alternative approach for fingerprint based authentication mechanism. By Shankar and Eswaran (2015) 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).

Linju and Mathews (2016) in this 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 pre-processing stage employments the basic piece substitution strategy and the halftone pictures are pre-processed utilizing SBR procedure. Hence, forth these are changed over into pre-processed pictures.

Proposed research: The main objective of the proposed research research 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 encrypt 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

MATERIALS AND METHODS

Proposed methodology has been divided into 2 phases:

- Image encryption
- Image decryption

Image encryption: In this image encryption phase, image is encrypted at multiple levels by using multiple shares. It must be colour 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 3 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 (Fig. 1-3).

Image decryption: The image decryption method research 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 9 shares are obtained. Each share from previous step decrypted into further shares to give 8 shares. The shares get stored in the data base for further decryption. The key is used to decrypt 8 shares of each colour to produce originally

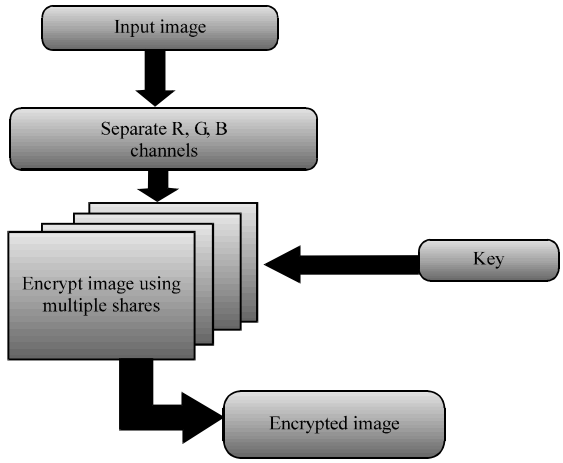

Fig. 1: Architecure of encryption

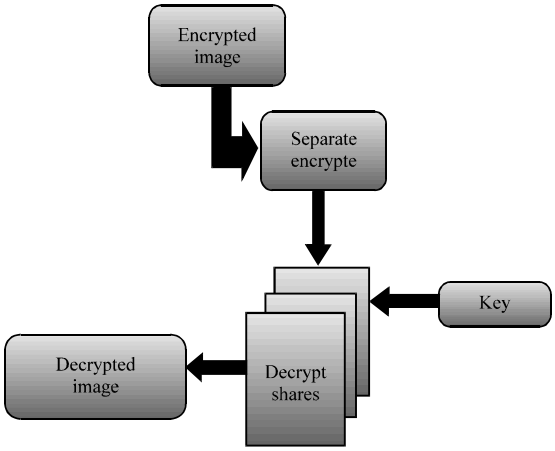

Fig. 2: Architecture of decryption

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. 4-8).

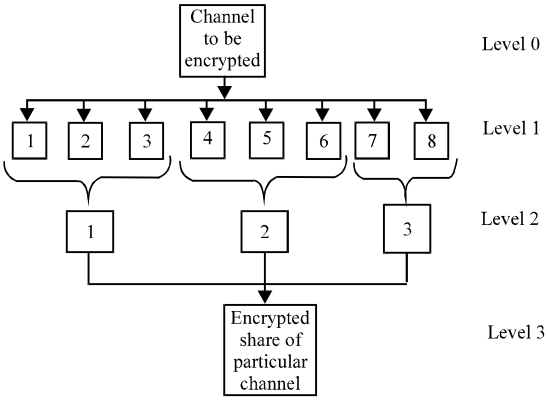

Fig. 3: Encryption of channel

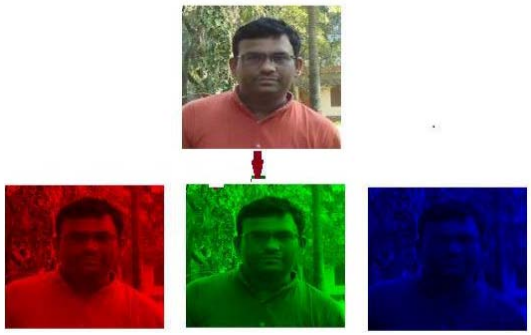

Fig. 4: Seperations of R, G, B channels

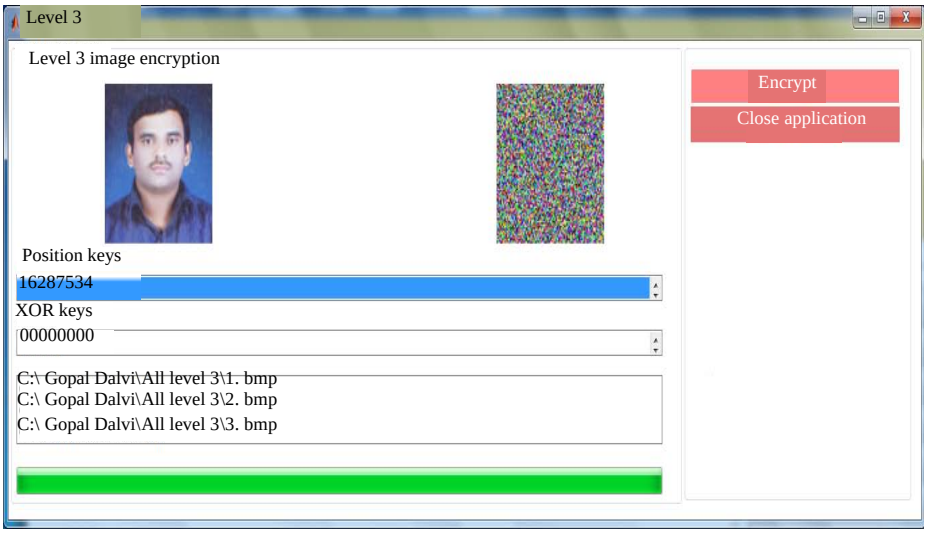

Fig. 5: Display GUI for image encryption (level 4)

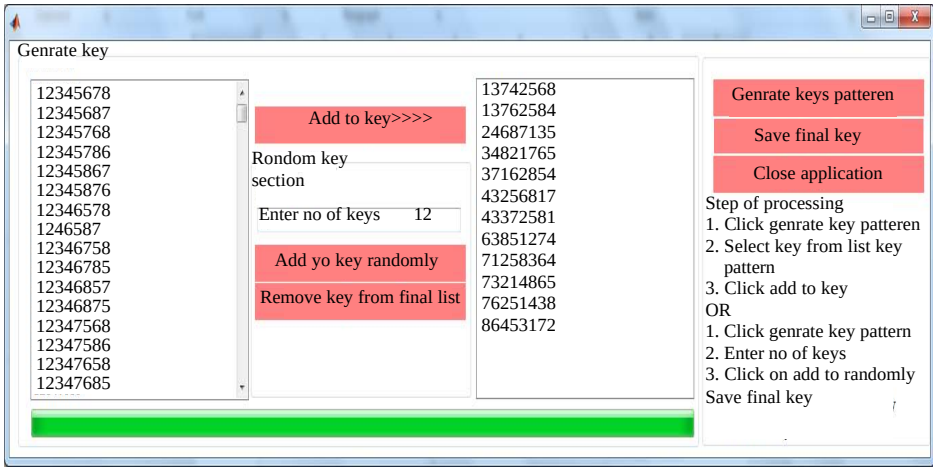

Fig. 6: Display GUI for selecting keys

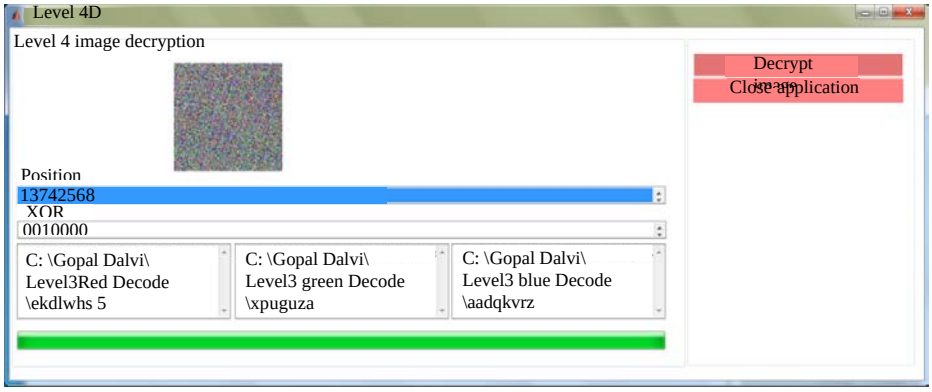

Fig. 7: Display GUI for image decryption (Level 4)

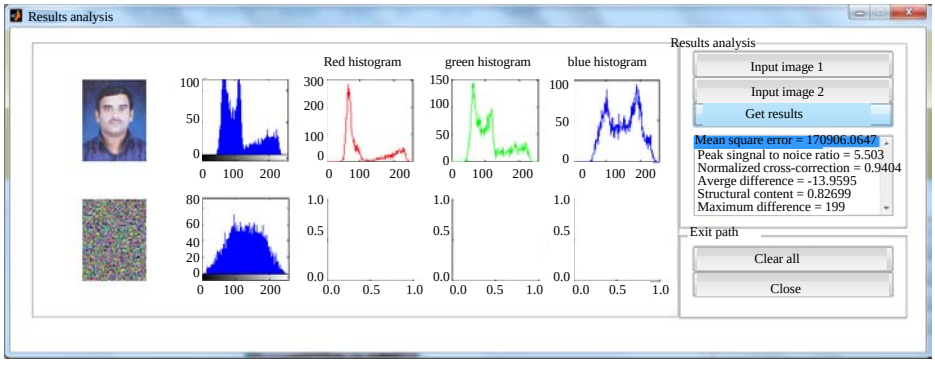

Fig. 8: Display of GUI for result analysis

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.

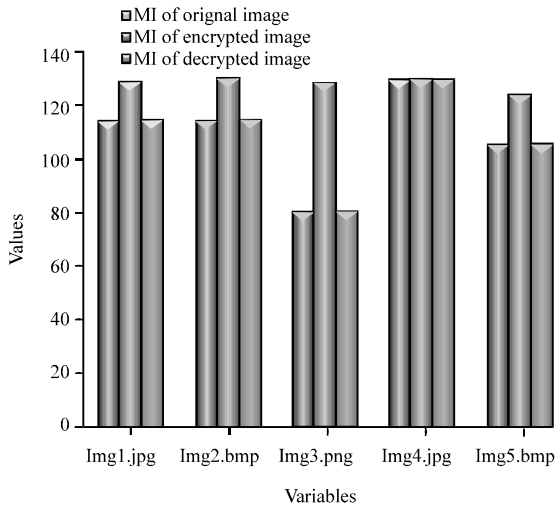

Fig. 9: Graph shows relation between mean intensity of original, encrypted and decrypted image

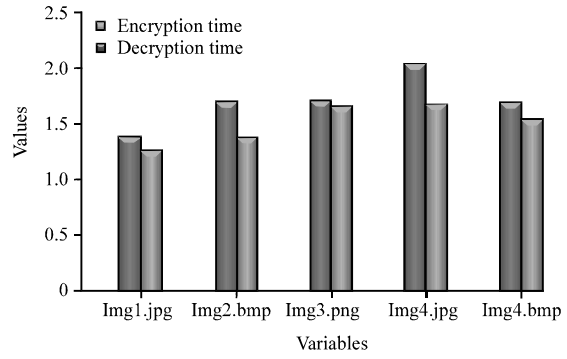

Fig. 10: Graph shows relation between encryption and decryption time required for level 3

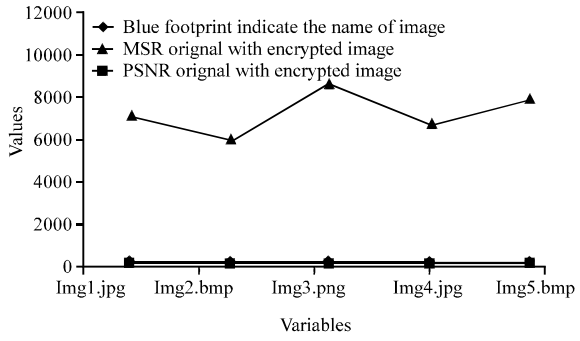

Fig. 11: Experimental result analysis

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:

Table 1: Comparison between mean intensity of original, encrypted and decrypted image

Input image	MI original image	MI encrypted image	MI 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: 2: comparison of encryption and decryption time required for level 3

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

$$PSNR = 10\log 10\ 2552\ MSE$$

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 (Table 1-2) (Fig. 9-11).

CONCLUSION

This study proposes a novel idea of facial image authentication using sterilization algorithm in VC. In this research 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.

ACKNOWLEDGEMENT

The researcher would like to thank S.G. Fale and other staff members of SGBAU for their valuable help.

REFERENCES

Dixit, S., D.K. Jain and A. Saxena, 2014. An approach for secret sharing using randomised visual secret sharing. Proceedings of the 2014 4th International Conference on Communication Systems and Network Technologies (CSNT), April 7-9, 2014, IEEE, Bhopal, India, ISBN:978-1-4799-3070-8, pp: 847-850.

Han, Y., W. He, H. Dong and J. Liu, 2012. A verifiable visual cryptography scheme based on XOR algorithm. Proceedings of the 2012 IEEE 14th International Conference on Communication Technology (ICCT), November 9-11, 2012, IEEE, Chengdu, China, ISBN:978-1-4673-2101-3, pp: 673-677.

Hou, Y.C., 2003. Visual cryptography for color images. Pattern Recognit., 36: 1619-1629.

Kang, I., G.R. Arce and H.K. Lee, 2011. Color extended visual cryptography using error diffusion. IEEE. Trans. Image Process., 20: 132-145.

Kaur, K. and V. Khemchandani, 2013. Securing visual cryptographic shares using public key encryption. Proceedings of the 2013 IEEE 3rd International Conference on Advance Computing (IACC), February 22-23, 2013, IEEE, Ghaziabad, India, ISBN:978-1-4673-4529-3, pp: 1108-1113.

Linju, P.S. and S. Mathews, 2016. An efficient interception mechanism against cheating in visual cryptography with non pixel expansion of images. Intl. J. Sci. Technol. Res., 5: 102-106.

Mande, A.U. and M.N. Tibdewal, 2013. Parameter evaluation and review of various error-diffusion half toning algorithms used in color visual cryptography. Intl. J. Eng. Innovative Technol., 2: 185-190.

Naor, M. and A. Shamir, 1994. Visual cryptography. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, May 9-12, 1994, Springer, Perugia, Italy, pp: 1-12.

Shankar, K. and P. Eswaran, 2015. Sharing a secret image with encapsulated shares in visual cryptography. Procedia Comput. Sci., 70: 462-468.

Thampi, S.M., 2008. Information hiding techniques: A tutorial review. BCs Thesis, LBS Engineering College, Kasaragod, India.

Verma, J. and D.V. Khemchandani, 2012. A visual cryptographic technique to secure image shares. Intl. J. Eng. Res. Appl., 2: 1121-1125.

Wang, R.Z. and S.F. Hsu, 2011. Tagged visual cryptography. IEEE. Signal Process. Lett., 18: 627-630.