Review Paper On Private Key With Share Key Of Variable Size Based Cryptographic Algorithm

1Ankit Pawar, 2Kamlesh Gehlot, 3Saloni Borate, 4Satlaj Thorat
1Student, 2Student, 3Student, 4Student
Dr. DY Patil college of engineering ambi pune

Abstract - **With the modernization of technologies, it's becoming quite easy to get private information from any person. Basically, VC is a secret message sharing method that uses distributed images as shares such that, when the distributed shares are stacked up, a concealed secret picture is revealed. No cryptographic computations are needed to decrypt the encryption images, rather it uses the human vision. In the existing visual cryptographic method during the creation of private key(mask key) automatically some changes are made in key data due to which during the time of decryption the quality of the picture decreases. In this paper, we proposed a new method of public and alter key encryption method for color images and without any pixel expansion which requires less space. In this method, all the changes made in the private key during creation are stored in the alter key for the decryption of images.**

keywords - **Visual Cryptography(VC), Halftone color images, Pixel Expansion, PSNR, Private key, Alter key**

I INTRODUCTION

In 1994 Naor and Shamir proposed the scheme of visual cryptography. This can be the crucial theme of visual cryptography within which the key image is split into two halves. Once the two shares are combined, it produces the first secret image. This pattern is merely for black & white pictures. Cryptography in general is a method used for securing information and communications using secret codes so that it can only be read by the person authorized to do so. In simple words, it defines a way of securely writing certain information in a hard-to-decode. With the use of hieroglyphics, Egyptians first used this technique back in 2020. Therefore, cryptography is important for the 3 security goals. 1. Integrity 2. Confidentiality 3. Availability Applications of visual cryptography 1. watermarking 2. Human-machine identification 3. CAPTCHA 4. Defense system 5. Anti-phishing system

II LITERATURE SURVEY

Cryptography is surrounded by much skepticism. There is progress being made in this area to remove skepticism. To increase the confidence in cryptography, the National Security Agency has joined with the National Institute of Standards and technology.Bhargav-Spantzel et.al deals with a recent paradigm in user-centric identity management. Bhargav-Spantzel states that, In relationship-focused identity management, the customer only maintains relationships with the identity providers. In credential-focused identity management, the customer must obtain long term credentials and store them in a local provider database. Bohli etal examined in their studies popular proof models for group key establishment and tools offered for scrutinizing group key establishment protocols in the presence of malicious participants. Bohli introduced that protocol proposed by Kim and Lee failed to offer a guarantee of security against a single malicious participant, whereas a protocol proposed by Katz and Yung in 2003 offers it. Tafaroji and Falahari introduced means of improving security data of code division multiple access. Three areas of a security vulnerability in software systems were analysed by the study of Yahav, Chandra,Fink and Pistoia. After doing analysis on the previous work in cryptography,we found that different techniques for cryptography have been discovered and many are yet to be revealed. Here, we are going to review an advanced method of information hiding.

III EXISTING SYSTEM

Countless approaches have been done for making the visual cryptography system more efficient than the existing one many different techniques had been used to improve the PSNR value, image quality, and to minimize data loss during encryption. Hence visual cryptography is the simplest method to share secret images and it is found by us that data loss still there in the existing visual cryptography model and during the encryption it is still affecting the PSNR value and resultant image quality.

IV PROPOSED SYSTEM

The method proposed is a method to encrypt a secret color image based on the VC systems. The images in secret color are encoded in parts of image without any meaning. Individual shared images do not provide information about the original secret image. The content of the secret image can be clarified only when stacking all shared images. The resulting shared image is of the same size as the original input image without pixel extensions

V SYSTEM ARCHITECTURE

1) Secret sharing using visual cryptography.

Step 1: Input image is given to the system.
Step 2: Encryption happens in this stage and key shares are created
Step 3: Decryption happens in this stage and the secret image is revealed
Step 4: Image output given back to the user

1:- Secret sharing system

VI ALGORITHM

The proposed method works in two stages: Decryption and Encryption

The Encryption Stage Algorithm

1. Create a Halftone image.
2. The halftone image is divided into three layers: red, green and blue.
3. Generate a randomly shared layer.
4. Creating a Key Share.

The Decryption Algorithm

1.Divide Encrypted Image into three layers:red, green and blue.
2. Stack each layer with mask.
3. Combine the resulting layer with a mask.
4. Decrypted Image is obtained.

VII Conclusion

Present and future era are certainly of advancement of Technology. As an instance, Cryptographic Computations are ordinarily required to decrypt the encrypted images. However, a novel Encryption technique is evolving having the potentials of using the Human vision to decrypt the encrypted images which is called as Visual Cryptography. In our research and in universal experiences Visual Cryptography was found to have the inherent defecta of pixel expansion. Through our project and research, we have introduced and suggested certain advanced methods to overcome this pixel expansion defect. Our project has also evolved with few techniques which will save most of the time required for computation and will also take very small space storage during the encryption process. For Example, to splitting shares are used for Encrypting an image viz... Key share and Random Share. The receiving side will receive the half tone image with random share and a generated Key share and there will be a private key used on both sending and receiving sides through which the random share will be generated. The Human Vision System after being exploited will reveal the Secrete color Image by stacking the two shares. This Proposed and enriched advance method will offer sound PSNR values compared to Visual Cryptography. In future, we are also taking an endeavor to improve this method through hard research and project.

REFERENCES

[1] Kumar, M.S., Shilpa, A. and Vijayalakshmi, A survey on Visual Cryptography Techniques. International Journal of Application or Innovation in Engineering & Management from the Source IJAIEM, this paper is based on the Literature survey of various visual cryptography techniques.
[2] Dua R. and Singh, N. (2016) secured Visual Cryptography Scheme Using Meaningful Shares. International Journal of Innovation Research in Computer and Communication Engineering. This paper focuses on the literature survey of various visual cryptography techniques.

[3] Akshay Ganjanan Bhosale & Vikram Shripati Patil, Visual Cryptography Technique with improved Contrast. This paper focuses on the improving image quantity by increasing contrast.
[4] Shereen, A. and Lijina. An Extended Visual cryptography scheme without Pixel Expansion Using Dithering. International Journal of Advanced Research in computer and communication Engineering, IJCNC. This Paper focus on Extended Visual Cryptography to improve the quality of recovered image.
[5] Saraireh,S. A Secure Data Communication System Using Cryptography and Steganography. IJCNC. This paper is focus on security using both cryptography and steganography.
[6] Rola I. Al-Khalid1, Randa A. Al-Dallah2, Aseel M. A secure Visual Cryptography Scheme using private key with invariant share sizes. Scientific research publishing. This paper focus on VC based on private key
[7] Jyoti Tripathia, Anu Saini, Kishan , Nikhil , Shazad. Enhanced Visual Cryptography: An Augmented Model for Image Security. ICCIDS. This paper is focused on less computational time during decryption process.
[8] Poonkuz hali1, S.M and Therasa, M., Data Hiding using Visual Cryptography for secure Transmission, IJARCCE, this paper is focus on hiding data using steganography technique.
[9] Sankar Das, Asoke Nath, Aritijt Samanta, Abhishek Roy, Saptarshi Bhattacharyya, A secure approach for Data Hiding using Visual Cryptography, International Journal of Innovation Research in Computer and Communication Engineering, this paper focuses on Visual Cryptography using XOR technique.