Visual Cryptography based Secret Sharing System

Nidhi Chauhan [1], Rajat Singhal[2], Shweta Maurya[3], Himanshu Pandey[4], Prof. G.V. Bhole[5]

[1,2,3,4]Student, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India
[5]Professor, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India

---***---

Abstract - *Visual Cryptography is an efficient encryption method to conceal information in images so that it very well may be decrypted by the human visual framework. The benefit of the visual secret sharing can be achieved by utilizing its decryption procedure where with no complex cryptographic calculation encoded secret information is decoded by Human Visual System (HVS). Be that as it may, the encryption strategy needs cryptographic calculation to partition the image into various parts for sharing (let n). k-n secret sharing plan is an exceptional sort of Visual Cryptographic procedure where gathering of k shares is required out of n shares to uncover the secret information, less than k shares will results in no information which leads to the safety of secret information. In our paper we have proposed a k-n secret sharing system for color image. We have taken an image which is to be shared secretly. This image is encoded utilizing a key given by the sender on which recipient also agrees. Further, the encrypted image is partitioned into N divisions shares utilizing K N Secret Sharing Algorithm. These N shares can be disseminated at the same time, the end user needs just K of these divisions to produce the original image. After the original image is produced it is still encoded. The key which is utilized to encrypt the image initially is presently required again to decrypt it, along these lines giving an extra dimension of security.*

Key Words: Visual Cryptography, encryption, decryption, Secret Sharing, Information Security

1. INTRODUCTION

The word cryptography originates from the Greek words κρυπτο (covered up or secret) and γραφη (composing). Strangely, cryptography is an art of secret writing. Individuals consider cryptography the art of disfiguring data or information into clear incoherence in a way permitting a secret strategy for unmangling. The fundamental provision given by cryptography is capable to send data between members in a way that keeps intruders from understanding the secret information. This sort of cryptography can give different administrations, for example,

- integrity checking—consoling the beneficiary of a message that the message has not been modified since it was produced by a real source.
- validation/ authentication—checking somebody's identity.

Visual cryptography is a prominent solution for image encryption by isolating the original image into transparencies. Visual cryptography was proposed in 1994 by Naor and Shamir who presented a basic however secure way that permits secret sharing with no cryptographic calculation, which they named as Visual Cryptography Scheme (VCS) [1]. Utilizing secret sharing ideas, the encryption system encrypt a secret image into the shares(printed on transparencies) which are commotion like secure images which can be transmitted or dispersed over an unbound correspondence channel. The least difficult Visual Cryptography Scheme is given by the possibility of a secret image comprises of an accumulation of high contrast pixels where every pixel is dealt with autonomously [3]. There are numerous calculation to encode the picture for sending purposes, however a couple of them have been in visual cryptography for color image. In this paper, the diverse methodology has been delivered for the visual cryptography for color image, the proposed system parts a secret image into n shares. We present the issue under thought and present the proposed calculation and building of new calculation is clarified alongside the test results are talked about in detail. Our system gives a choice to the end user of encryption. The end user can divide the original picture into desired number of shares along with the desired number of shares need by end user to get the secret information. Utilizing our system, we can send encrypted images that are can be saved in the machine and can be sent to the expected individual by different methods [source].

1.1 History/Background

All together for the benchmarking plan to be legitimately created and executed, a designer needs a consciousness of the historical backdrop of Visual Cryptography. The developer likewise needs a comprehension of the fundamental ideas of Visual Cryptography and how they are utilized to create shares of encrypted images. As of late, Visual Cryptography has been reached out to oblige shares of grey and colored images, further expanding its abilities and flexibility. This comprehension of Visual Cryptography is important to permit a target correlation of all the distinctive sorts of algorithms.

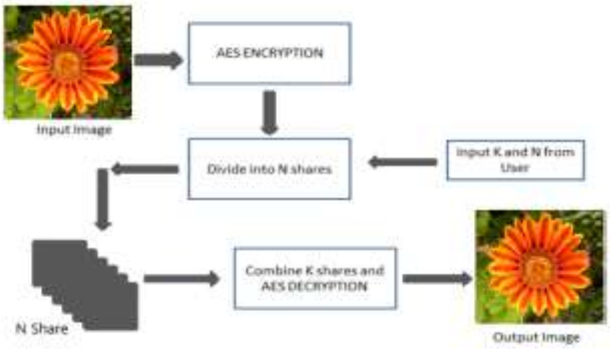
The field of Visual Cryptography has advanced in the course of recent years. The main Visual Cryptography technique was presented by Moni Naor and Adi Shamir in 1994. Their paper concentrated on a procedure for impeccably encoding digital media that could be decoded utilizing exclusively the human visual framework. This thought would enable written material to be carefully transmitted without worry that the message could be captured and inadvertently uncovered to unapproved parties. The essential depiction related with Visual Cryptography is the message being encoded into two shares. At the point when taken a gander at separately, these shares uncover no data about the message contained in them and look like irregular noise-like pattern. Be that as it may, when these shares are imprinted on transparencies, overlaid, and carefully adjusted, the message contained in the shares is uncovered. The message is uncovered without extra estimation or control. This component guarantees that the safe procedure can be utilized by somebody who has no past learning of Visual Cryptography, programming foundation, or cryptographic analysis experience.

2. LITERATURE SURVEY

In [1], Naor and Shamir presented VCS and suggested a few developments, where the universal one supports k out-of-n limit setting for black-and-white images . The scheme they proposed does not support images of random number of colors. A VCS has less pixel expansion when contrasted with [1] was proposed by Adhikari et al. [4]. In [5], Yang proposed a scheme which accomplishes negligible pixel expansion however that supports only black-and-white images . Chen et al. proposed another model which stretched out the outcomes to gray-scale images and presented a gray-scale VCS [6] with no pixel expansion. Nonetheless, their scheme does not support the generic k-out-of-n threshold setting. Likewise, it additionally needs to carry out square averaging (for example preprocessing) on the original image prior completing the secret sharing. Another gray scale VCS without pixel expansion was proposed by Chan et. al [7] . Their scheme likewise needs preprocessing by fluctuating and changing the dim dimension of the original image. Their model as not bolsters the generic k-out-of-n threshold setting. . Hou's plans [8] are viewed as the primary arrangement of color VCS'. For color VCS, we can allude [8-13], All the schemes in [8] are having the pixel extension of 4 and don't bolster the general k-out-of-n threshold setting and fluctuation is required for preprocessing the native image. Yang and Chen proposed a VCS for colored images dependent on an added substance shading blending strategy [13]. In their plan, every pixel is extended by third factor. Hou and Tu proposed another color VCS [14]. The scheme additionally bolsters k-out-of-n threshold setting with no pixel development. Dithering is as yet required for preprocessing the generic image before secret sharing. Shyu proposed an effective c-color (k, n) edge visual secret sharing scheme [15] and has furthermore enhanced the pixel expansion keeping the great visual quality of the uncovered secret images. In [16] Wu et.al. Presented a feasible procedure for accomplishing zero pixel expansion and conventionally changes over any k-out-of-n edge visual cryptography plot for black and white images into one supporting color images. Dastanian [20] presented another visual cryptography conspire, able to transmit the two secret images with the utilization of two shares. With arranging two offers, secret image I shows up and with assembling one of the share with 90 degrees pivot in clockwise on other share shows up the secret image II.

3. PROPOSED SYSTEM

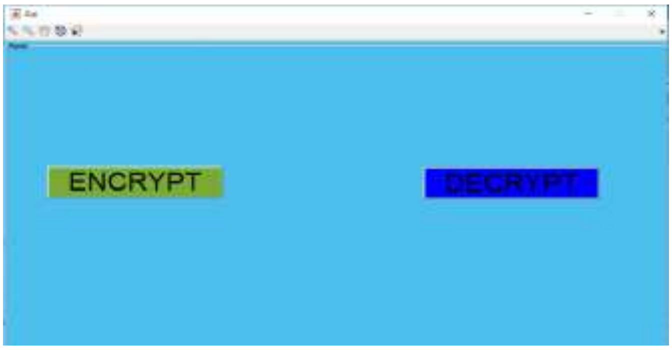
In this system, we have take an image which is to be shared secretly from one machine to another or as desired. This image is encrypted using a strong password given by the sender as key. Moreover, this encrypted image is partitioned into N different shares using K-N Secret Sharing Algorithm. These n shares are then distributed but the recipient needs only k shares out of these n shares generated to get the original image. This original image generated still remains in encrypted form. The password (or key) which is used to encrypt the image at the sender end is now required again by the recipient to decrypt it, thus providing a certain level of security in transmission which is needed to protect the sensitive data from manipulation by intruders.



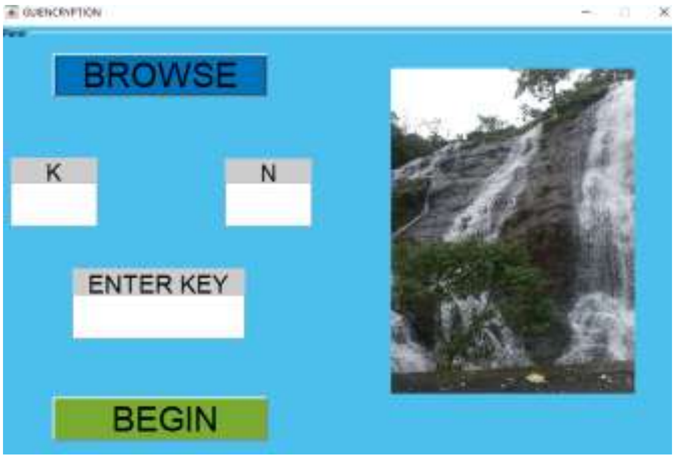
3.1 Graphical User Interface

GUI for the program is made utilizing Matlab 2018a. It has every one of the functionalities required for Encryption and Decryption of secret image to be shared. Following are the means to run the GUI:-

Step 1: This is the main screen of our proposed system.



Step 2: To start the encryption process click on "Encrypt" button, below screen will popup.



Step 3: Click on "Browse" button to select the image you want to share secretly from file selector. Now start filling the values of k, n and to encrypt the image enter a password as key for encryption process. Click on "begin" button.

The shares generated will get stored in current Matlab directory.

Step 4: For Decryption process at the recipient end, Click on "decrypt" button of the main screen. A screen will popup for decryption where the recipient has to enter the number of shares available at his side along with the key that had been chosen by the sender. Entering wrong key will result in another noisy image, which the recipient will not be able to decrypt.

Step 5: After following the above steps, the recipient will get the decrypted image which is the exact duplicate of original image.

4. CONCLUSION

The system proposed in this paper has been tried on different types of colored input images by observing changes in size and key for encryption algorithm. The whole time secret image is recovered with great visual quality. As the image processing takes place on key images and its shares, there is no noticeable change in the quality of decrypted image at the recipient end. The k-n secret sharing system proposed in this paper partitioned the original image into n shares such that at least k shares are required at the recipient end for decryption process without compromising with quality of decrypted image. As future work, this system can be modified to incorporate the encryption of multiple colored images and generate their shares at once rather than encrypting single colored image at a time. Increasingly complex public key encryption can be utilized to minimize key size. Image processing assaults like interpretation, pivot and scaling of key shares can likewise be controlled to some extent.

REFERENCES

1) M. Naor and A. Shamir, "Visual cryptography," in Proc.AdvancesinCryptography(EUROCRYPT'94), 1995, vol. 950, LNCS, pp. 1–1

2) Talal Mousa Alkharobi, Aleem Khalid 2003. New Algorithm For Halftone Image Visual Cryptography, Alvi King Fahd University of Pet. & Min. Dhahran.

3) JIM CAI 2003. A Short Survey on Visual Cryptography Schemes

4) A. Adhikari, T. K. Dutta, and B. Roy, "A New Black and white Visual Cryptographic Scheme for General Access Structures", in Progress in Cryptology - INDOCRYPT2004, 2004, pp. 399-413, Lecture Notes in Computer Science,3348.

5) C. N. Yang, "New Visual Secret Sharing Schemes Using Probabilistic Method", Pattern Recognition Letters, 25, No. 4, pp. 481-494, March 2004.

6) Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, and Y. P. Chu, "A multiple-Level Visual Secret-Sharing Scheme Without Image Size Expansion", Information Sciences, 177, No. 21, pp. 4696-4710, November 2007.

7) C. S. Chan, Y. W. Liao, and J.C. Chuang, "Visual Secret Sharing Techniques for Gray-Level Image Without Pixel Expansion Technology", Journal of Information, Technology and Society,95, No. 1, 2004.

8) Y. C. Hou, "Visual Cryptography for Color Images", Pattern Recognition, 36, pp. 1619-1629, 2003.

9) R. Lukac and K. N. Plataniotis, "A Cost-Effective Encryption Scheme for Color Images", Real- Time Imaging, 11, pp. 454-464, 2005.

10) S. J. Shyu, "Efficient Visual Secret Sharing Scheme for Color Images", Pattern Recognition,39, No. 5, pp. 866880, 2006.

11) C. N. Yang and T. S. Chen, "Reduce Shadow Size in Aspect Ratio Invariant Visual Secret Sharing Schemes using a Square Block-Wise Operation", Pattern Recognition,39, No. 7, pp. 1300-1314, 2006.

12) S. Climate, R. D. Prisco, and A. D. Santis, “Colored Visual Cryptography Without Color Darkening”, Theoretical Computer Science, 374, pp. 261-276, 2007.

13) C. N. Yang and T. S. Chen, “Colored Visual Cryptography Scheme Based on Additive Color Mixing”, Pattern Recognition,41, No. 10, pp. 3114-3129, 2008.

14) Y. C. Hou and S. F. Tu, “A Visual Cryptographic Technique for Chromatic Images Using Multi-Pixel Encoding Method”, Journal of Research and Practice in Information Technology,37, No. 2, pp. 179-191, May 2005.

15) S. J. Shyu, “Efficient Visual Secret Sharing Scheme for Color Images”, Pattern Recognition,39, pp. 866- 880, 2006.

16) Xiaoyu Wu, Duncan S. Wong, and Qing Li “Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion”, Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT ’09) Huangshan, P. R. China, 26-28, Dec. 2009, pp. 310-31.

17) Ching-Sheng Hsu and Shu-Fen Tu, “Digital Watermarking Scheme with Visual Cryptography”, Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol IIMECS 2008, 19-21 March, 2008, Hong Kong.

18) Chandrasekhara & 2Jagadisha, Secure Banking Application Using Visual Cryptography against Fake Website Authenticity Theft, International Journal of Advanced Computer Engineering and Communication Technology (IJACECT), ISSN (Print): 2278-5140, Volume-2, Issue – 2, 2013.

19) Mr. K. A. Aravind, Mr. R .Muthu Venkata Krishnan, Anti-Phishing Framework for Banking Based on Visual Cryptography, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January-2014.

20) Rezvan Dastanian 1and Hadi Shahriar Shahhoseini “Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares”, International Conference on Information and Electronics Engineering IPCSIT 6 (2011) pp. 171-175.