Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 6 (2017), pp. 2555-2561
© Research India Publications
http://www.ripublication.com

Visual Cryptography for Color Images to Provide Confidentiality Using Embedded System

SindhuParkavi.S[1], Sharon.I[2] and Prof. S. Gowri[3]

[1, 2]Department of Information Technology, Sathyabama University, Chennai, India.
[3]Professor, Department of Information Technology, Sathyabama University, Chennai, India.

Abstract

RGB Color Visual Cryptography is a type that allows the image to be divided into 2*2 (n*n) multiple numbers of shares knows transparent shares. In existing methods works for color images with 8 colors and even few of them without halftone techniques. Today as per the growth of digital media in world, it is becoming more prevalent to find a method to protect the security of that digital media. We present a visual cryptographic technique for color images in which the generated shares (n*n) are again encrypted. For this XOR operation is used and this will provide double security for the secret document. There is no pixel expansion and hence storage requirement per encrypted image is same as original image without pixel expansion. Encryption is carried out based on RGB (HSV) value of the pixels. Encryption is carried out based on RGB value of the pixels. The quality of the image recovered is same as the original image. The same technique can be used on binary or gray scale images also without any change in the algorithm. RBG Color Visual Cryptography is an exciting era of research where exists a lot of scope.

Keywords: Visual Cryptography, (key, 2, 2) Visual cryptographic scheme, Encryption, Contrast, Shares, Pixels, Secret sharing, stacking.

I. INTRODUCTION

Presently days, data sharing and exchange have been expanded quickly. Along these lines, there is risk from outsider or unapproved party getting to mystery data has been an always existing sympathy toward the information correspondence specialists. Many secure and classified information things like military maps and business recognizable pieces of proof are sent over the web. While utilizing mystery reports (pictures, content and so on.) for sending over the system, the security issue is to be contemplated, since there is a shot of taking the mystery data by the programmers

because of powerless connection in the general population organize. So as to manage the security issue of mystery pictures, we need a fitting secure calculation by which we can secure our information over the web. With the assistance of Visual Cryptography, the framework visual data can be safely sent over the web. [1] This article is an arrangement with the Review investigation of RBG-shading visual cryptography there is a requirement for study. In the study of RBG CVCS (Color visual cryptography) mathematical techniques related aspects of information security such as data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. This technique is based on Human Visual System and hence do not include complex mathematical computations. In this scheme, (k, n) (VCS) Visual Cryptography Scheme for color images(RBG) in technology as HSV is described with c colors as a collection of c subsets in nth Cartesian product of the finite lattice.The proposed scheme is more secure and it is very easy to implement with low computation cost. In this proposed scheme, Very first the secret image is taken and then it is divided into shares after converting it into binary image, next the shares of binary image are encrypted and decrypted by using RSA algorithm, because of this even if the unauthorized person, once getting all the shares, he/she can't get back the original secret image without availability of the private key.

II. RELATED WORK

In halftone VC a secret binary pixel is encoded into an array of sub pixels [5], referred to as a halftone cell, in each of the shares this is for a Binary image. Halftone method is nothing but a breaking the pixel into white and black and creating the share for each pixel then overlaying the each share to get an original image. For color image we have to fix the threshold value while breaking the pixel [9][10]. Threshold value can be fixed according to bit level, color pixel has three byte, and these three bytes average value is used to fix the threshold value in a halftone method. First it takes average value of all three colors then it fixes the threshold range for each particular color.

Kulvinder Kaur, Vineetha Khemchandani told about the VCS is a sender transmits the secret image which is divided into shares and it holds hidden information. Consequently, the secret image information cannot be retrieved from any one transparency via human visual perception. Both author Ching-Nung Yang, Tse-Slih Chen say about VCS is visual cryptography scheme (VCS) encodes a secret image into n shadow images (shadows) distributed among n participants.

Recursive hiding of secrets was first introduced by M. Gnanaguruparan and Subhash Kak [5], with applications to both images and printed text, to increase the efficiency of visual cryptography and to make it possible to incorporate additional secret information that serves as a steganographic channel [6]. The idea involved in recursive hiding of secrets is that several multiple messages can be hidden in one of the shares of the original secret image. The secret images that are to be hidden are taken according to their sizes from the smallest to the largest (i.e., secret size doubling at every step). The smallest secret image is divided into n shares using the basic idea of visual cryptography. These n shares are placed below each other, and they now represent the first share of the secret image. The second share is accomplished in such

a manner that if the n shares are overlaid, then the secret image is revealed under consideration. Important thing to be noticed is that the share of the original secret image that contains the recursively-hidden information must also contain both the shares of the last hidden secret image [5]. .

III. SYSTEM OF PROPOSED SCHEME

In the proposed strategy, the RGB (Red, Green and Blue) shading picture is taken for the data sharing. For the mystery picture sharing and afterward stacking the decoding is included. By utilizing the proposed strategy, the force of the first picture is kept up and in addition 16 shares can be made and utilized. This segment comprises of the calculation for the share era in the shading models. In the current strategies the added substance and the subtractive shading models were utilized to halftone or to deliver the nonstop shares and the stacked pictures. Then using the CMY model around standard 8 color codes was generated. The proposed algorithm uses the basic RGB color.In the proposed method, the RGB (Red, Green and Blue) color image is taken for the information sharing. For the secret image sharing and then stacking the decryption is involved. By using the proposed method, the intensity of the original image is maintained as well as 16 shares can be created and used. This section consists of the algorithm for the share generation in the color models. In the existing methods the additive and the subtractive color models were used to halftone or to produce the continuous shares and the stacked images. Then using the CMY model around standard 8 color codes was generated. The proposed algorithm uses the basic RGB color.

IV. SYSTEM ARCHITECTURE

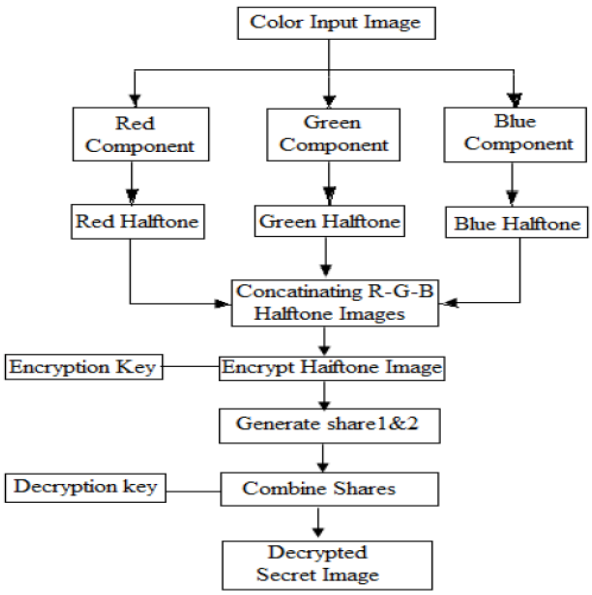

Fig 1 overview of system architecture

In this paper, the quantity of pixel in the decoded picture is same as in the first mystery. Subsequent to testing on a wide range of pictures the outcomes are as our desire and the shares are clear with no visual variation from the norm. This strategy can work for both shading pictures and also dark scale pictures. All that is required is to transmit key on a mystery channel while encoded frame can be transmitted on an unsecure channel.

V EXECUTION MODULE FOR VISUAL CROPTOGRAPHY

1. Interface configuration utilizing Applet outline work

In this module, we plan UI configuration utilizing applet outline work. The UI ought to be simple and reasonable to each client. So that any one can get to utilizing our framework. It must be supportable utilizing different GUIs. The UI additionally comprises of help record. The help record helps on each ideas of the implanted visual cryptography. Help document ought to obviously portray the subtle elements of the venture created in straightforward dialect utilizing different screen shoots.

2.Visual Cryptography Implementation

Every pixel of the picture is partitioned into littler squares.On the off chance that the pixels of layer 1 and 2 are altered or inverse, the exaggerated rendition will be totally dark. This is a data pixel [7].This module is the center for the venture, where we execute the Visual Cryptography. We utilized LZW Data Compression calculation. The LZW information pressure calculation is connected for the dim scale picture here. As a pre-handling step, a lexicon is set up for the dark scale picture. In this lexicon, the string replaces characters with single quotes. Figurings are done utilizing dynamic Huffman coding. In pressure of grayscale picture select the data pixels. At that point produce halftone offers utilizing blunder dissemination strategy. Finally channel process is connected for the yield dim scale pictures. Channels are utilized to enhance the nature of reproduced picture to limit the clamors for honing the information mystery picture.

3. Encoding Module

This Module is used to encrypt the image. That is we are going to divide 1 image into many number of pixels. Here we are using an algorithm which is mentioned below. Also we are creating a dictionary to store the image or strings.Initialize the lexicon to contain all strings of length one. Find the longest string W in the lexicon that matches the present info. Emit the word reference file for W to yield and expel W from the information. Add W took after by the following image in the contribution to the word reference. A word reference is introduced to contain the single-character strings comparing to all the conceivable info characters (and nothing else aside from the reasonable and stop codes in the event that they're being utilized). The calculation

works by looking over the information string for progressively longer substrings until it discovers one that is not in the word reference.

4. Decoding Module

The deciphering calculation works by perusing an incentive from the encoded input and yielding the relating string from the instated word reference. In the meantime it acquires the following an incentive from the info, and adds to the word reference the connection of the string simply yield and the principal character of the string got by disentangling the following information esteem. The decoder then continues to the following info esteem and rehashes the procedure until there is no more contribution, and soon thereafter the last information esteem is decoded with no more augmentations to the lexicon. Along these lines the decoder develops a lexicon which is indistinguishable to that utilized by the encoder, and utilizations it to decipher consequent info values. Along these lines the full word reference does not need be sent with the encoded information; simply the underlying lexicon containing the single-character strings is adequate (and is normally characterized in advance inside the encoder and decoder instead of being unequivocally sent with the encoded information.)

5. Creating Transparencies Module

This plan gives hypothetically idealize mystery. An aggressor who acquires either the straightforwardness picture or the screen picture gets no data at about the encoded picture since a dark white square on either picture is similarly prone to encode a reasonable or dull square in the first picture. Another profitable property of visual cryptography is that we can make the second layer in the wake of disseminating the principal layer to deliver any picture we need. Given a known straightforwardness picture, we can choose a screen picture by picking the proper squares to deliver the coveted picture. A standout amongst the most evident impediments of utilizing visual cryptography in the past was the issue of the decoded picture containing a general dim impact because of the extra dark sub pixel from encoding. This happened in light of the fact that the decoded picture is not a correct preproduction, but rather an extension of the first, with additional dark pixel. Dark pixel in the first record stays dark pixel in the decoded rendition, yet White pixel gets to be distinctly dim. This brought about a considerable measure of difference to the whole picture. The additional dark sub pixel in the picture causes the picture to wind up distinctly contorted.

VI. CONCLUSION

In existing visual Cryptography situation, there exists low security for shares made. Not at all like most investigations of visual cryptography, this paper abuses the systems of dithering innovation and shading deterioration to build 16 shading code models from standard RGB. To defeat the impediments of existing strategies, the

proposed technique develops a 16 shading code instrument which is more fitting to secure the shares. The proposed technique can be enhanced by cultivating the hues made and to deliver clear resultant picture. The calculation fortifies the security by producing more number of hues to create offers. The test comes about uncover that the proposed plot guarantees best reproduction of pictures with attractive quality because of the tunable element in the mystery share creation step Any individual having adequately k number of shares can without much of a stretch recreate the first picture. In a future endeavor we need to give some security plans to the proposed method to make the plan more secure.

REFERENCES

[1] Secure Visual Cryptography Scheme for Sharing Secret Image using RSA Siddaram Shetty1, Minu P Abraham2 PG Scholar, Dept. of CSE, NMAMIT, Nitte, Udupi, Karnataka, India1 Asst. Professor, Dept. of CSE, NMAMIT, Nitte, Udupi, Karnataka, and India.

[2] G. R. Blakley. Safeguarding cryptographic keys. In Proceedings of the National Computer Conference, volume 48, page 313C317, 2009..

[3] J. Ida Christy and Dr. V. Seenivasagam, ”Construction of Color Extended Visual Cryptographic Scheme Using Back Propagation Network for Color Images”, 20 12 International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 978-1-4673 -02 1 0-41 1 2©20 12 IEEE.

[4] Kai-Hui Lee and Pei-Ling Chiu.”An Extended Visual Cryptography Algorithm for General Access Structures,”ieee transactions on information forensics and security, vol.7, no.1, February 2012,

[5] Weir J., Yan W. Q., Sharing Multiple Secrets Using Visual Cryptography, IEEE, 2009

[6] Y. Bani, Dr. B. Majhi and R. S. Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique.In Proceedings of 2nd National Conference, IndiaCom 2008.

[7] Mandal, J.K.; Ghatak, S. A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography (SCOSVC), Electronic System Design (ISED), 2011 International Symposium on, On page(s): 329 – 334

[8] Mandal, J.K.; Ghatak, S. Secret image / message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC), Recent Trends in Information Technology (ICRTIT), 2015 International Conference on, On page(s): 263 – 268

[9] Katta S., Recursive Information Hiding in Visual Cryptography, 2010

[10] Yue T. W., Chiang S., A Neural Network Approach for Visual Cryptography. Proceedings of the IEE-INNS-ENNS International Joint Conference on Neural Networks(IJCNN‟00) .pp. 1-2. 2015

[11] Chakraborty U., Paul J. K., Mahapatra P. R. S., "Desigan and Implementaion of a (2,2) and a (2,3) Visual cryptographic scheme". IJCCT Vol.1 Issue 2,3,4; 2010 .

[12] W.-G. Tzeng and C.-M. Hu, "Anewapproach for visual cryptography, "Designs, Codes, Cryptog. vol. 27, no. 3, pp. 207– 227, 2002.

[13] M. Naor and A. Shamir "Visual cryptography: Improving the contrast via the cover base" IACR Eprint archive, 2011

[14] C.-N. Yang and C.-S.Laih, "Some new types of visual secret sharing schemes," in Proc. Nat. Computer Symp., 2015, vol. 3, pp. 260–268.

[15] Pei-Yu Lin, Ran-Zan Wang, Yu-Jie Chang, Wen-Pinn Fang," Prevention of cheating in visual cryptography by using coherent patterns", Elsevier on Displays,301(2015), 61-74