Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Sharing Colour Images Using Extended Visual Cryptography (EVC) With Expansionless Shares

Mrs. G.Shoba*, Ms. K. Anitha, Ms. S. Banupriya, Ms. D. Lalitha
CSE & Pondicherry University,
India

Abstract— Visual cryptography is an encryption technique to send image, video, etc. We propose a new visual cryptography scheme that hides the secret of the original colour image by using digital half toning technique. It is done by embedding the colour image into the grey scale image. This scheme help us to send the embedded image by using multiple shares through multiple channels. Half toning with error diffusion helps to improve the quality of the image. Secret information can be retrieved by stacking any k number of decrypted shares which reduces the colour sets that renders the halftone image and chooses the colour whose brightness variation is minimal.

Keywords— EVCS, encryption, digital half-toning, decryption

I. INTRODUCTION

In the multimedia era, all the information are send through the internet globally. With the availability of global networks the digital media has grown widespread. Digital information like audio, video, images, documents have been in great use in the fields of education, research, entertainment, media and military. This is made easy because the digital information can be captured, stored, modified and transmitted as needed. However, with these tremendous improvements in digital computer technology there are some issues. The main problem is, it is becoming unsafe to transmit the secret images such as military maps or commercial images. The malicious hackers may listen to the internet and try to steal these secret information. Visual cryptography is introduced to provide secure transmission multimedia information through the internet.

A. Traditional Visual Cryptography Scheme

Traditional visual cryptography scheme is the first visual cryptography introduced by Naor and Shamir[1] in the year 1995. This technique helps in concealing the secret information present in the image that is being transmitted. The traditional visual cryptography method encodes the original binary image into number of shares. The shares are generated in such way that some shares may contain the random pixel arrangement while the other share contain the secret information to be delivered. An encoded image or a share will reveal nothing about the secret information. When all the shares are superimposed the original information is revealed.

II. RELATED WORK

Visual Cryptography (VC) is not enough to provide meaningful shares of coloured images with high quality of the picture. This paper produces visual cryptography encryption method for colour images in any standard format and uses the error diffusion technique to create meaningful shares with high quality. As it minimizes the lower frequency differences of input and output images, it is possible to generate halftone shares that are meaningful to the human visual system. The contrast between the shares are improved with synchronisation across colour channels. [2]

With express growth in the field of network, Internet has become the principal source of transmitting the very confidential information like business documents, military information, etc. In such situations, the techniques that are intended to protect these in information play a vital role in supply of trust and easy transmission over the internet. Visual cryptography is one such sheltering technique that helps in transmission of secret visual information in an effective way. There are several encryption algorithm one such includes Shamir, Blakley and Asmuth-Bloom to distribute the images into number of cleaves called shares. The sharing lead to high computational complexity and the shares generated are noisy images which are meaningless that causes suspicion. Later creating meaningful shares scheme was introduced by Lin and Tsai but it has the same computational complexity problem. To subdue all the above problems a new technique called steganography with encryption done with symmetric key that produces the meaningful shares. This pays a solution to all authentication challenges of the current situation. [3].

Visual cryptography schemes (VCS) are an extraordinary secret sharing scheme where the image to be send is the secret. For a set of P, a VCS encrypts a secret image into n number of transparencies. Then n transparencies are given to the n participants. The set of participants are cleaved into qualified sets and forbidden sets. The qualified set of participants can reveal the visual stack by simply stacking their transparencies while the forbidden sets have no information about the concealed image. The impression of visual cryptography proposed by Naor and Shamir suggest the pixel expansion of k out of k of image to be at least 2k-1. Also they have a grant an image of k out of k design with pixel enlargement 2k-1.[4].

III. EXISTING SYSTEM

The existing VCS adopt the digital visual secret sharing technology and range the dusky shade of the image in correspondence to the digital halftone technique that creates an encoded image for security. Three constructions are used:

- Construction1 is an increase of Naor and Shamir's (2,2)-VCS
- Construction 2 is a (k,n)-VCS
- Construction 3 is a (2,2)-VCS

These two constructions loosen the oppositionpredicament of VCS to correct the opticproperty of shadestopessentially. However, the halftone engravinghideidolstay on a remodelshow and abate the clarity of a secluded. VCS which uses grizzliness to characterizeakind from innocenthide. A dusky-and-favourablereconditecopy is division into report-copydarkness by redivide a secluded pixel into m (appeal to as the pixel dilation) hoagie pixels in each of n shade. VCSs with specifyingshape, such as cleavemanifoldconcealed, deceptionpreclusion, explanation misalignment proposition, perform the fancifulcomparison, carevisionrateinvariable, portiongrey-headed/kindcaststipulatecircuitrevival, furnishrankadditioncharacteristic, and speechlessersupported VCS.

A. Limitations of the Existing System

VCSs have random arrangement of pixels in the transparencies, which are doubted to critic and troublesome for identification and care. It will be performance on two cloudygradationhidecopy which generate the same grizzleblushlook. The confidenceconclusion is a cruciformproposition in the transmission progress.

IV. PROPOSED SYSTEM

Visual cryptography scheme is one of the most secure techniques for privacy protection, that allow the encryption of secret image of data cleaving it into the secure image shares or data and transferring it into the secure channel and this scheme is able to reveal the original image without any computational complexity. In current era, security of the transmitted data is very important issue as the network technology is widespread and all the confidential information are send through the internet.

We propose a new scheme in which the secret image to be transferred is the colour image which is enveloped by the grey image scale image that would confuse the malicious hackers. The embedded image is then processed to produce the shares. The shares are generated without any pixel enlargement that reduces the space complexity. This is done by using the hierarchical visual cryptography technique. At the receiver side the shares are stacked together and a key is used to remove the cover image and reveal the secret of the image.

A. Architecture Of The Proposed System

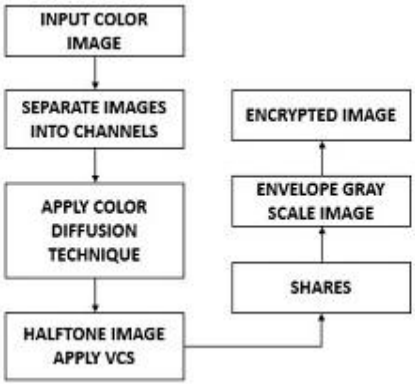


Fig. 1Encrypting the image at the sender side

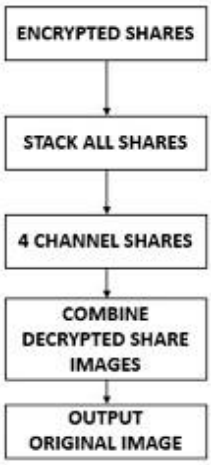


Fig. 2 Decrypting the image at the receiver side

B. Expansionless Shares In Visual Cryptography:

In formermanufacture of visual cryptography, we ciphered the latent with the dilationrate of 1:4 and posterior 1:2. The expansedenote that if inventivesecluded is of largeness AXB then with expanseproportion 1:4 the division have magnitude 4AX4B and with enlargementproportion 1:2 the dividendborrowed are found to be of adjust 2AX2B. Due to this enlargementhierarchicencoding of concealedgot affected. During cypheringsecond-hand HVC initially retired is encipheredworn 1:2 enlargementratebenefaction two cut S1 and S2. If S1 and S2 are coded with the same expanserate independently then the resulting four part are again widesystem of S1 and S2 (S1 and S2 are already wide in first flat of coding). This vastdilation in dividendassume the walkcomplication. While superpose the shear of HVC, the larger transparencies are need. Expansion-less hierarchicvisible cryptography is the discharge to lessen this expanse in the part. The requisition of this talkorder is that the private should be in twofigure i.e. dusky and pure passwords, signatures, manuscriptSMS etc. Before cipher, the genuineunknown is to adjust which is manifold of 4. Before inscribe the private, it is renormalize. The resize service of OCTAVE/MATLAB is to do any isolation whose greatness is manifold of 4. After resizing the secluded starting with top nearquarter of recondite every 2X2 pixel blockhead is selected for encoding independently. The encoding of 2X2 roof is done among changeablehaphazard combinations. If 2X2 blockhead in inventivesecluded is trulyinky then this blockhead is written in codesecond-hand 4 possibilities personate by equality 1 - 8. There are manifold possibilities for the 2X2 pixel stuff. The encoding combinations for share 1 of whole atrocious stuff of pixels are delineate as given in the below:

[1 0; 0 1] (1)
[0 0; 1 1] (2)
[1 1; 0 0] (3)
[1,1; 1 0] (4)

The encoding combinations look in share2 are fixed by:

[0 1; 1 0] (5)
[1 1; 0 0 (6)
[0 0; 1 1] (7)
[1 0; 0 1] (8)

Similarly, if 2X2 blockhead of secluded is found to be sincerelydarling then such blockhead is encoded with 4 violence combinations. Share1 of encoding for fortunatestuff of pixels is fixed by:

[0 0; 0 1] (9)
[0 0; 1 1] (10)
[1 1; 0 0] (11)
[0 1; 1 0] (12)

Above combinations also example share2 as the fundamentalcorrectness of encodepallid pixel specify that the design of share1 and share2 must be same. Third option for 2X2 pixel wall is neither innocent nor innocentpicture. In such accident the writing in code is done wornsucceeding combinations. Share 1 for force combinations is assumed below:

[0 1; 1 0] (13)
[1 0; 1 0] (14)
[0 1; 1 1] (15)
[1 0; 1 1] (16)

Corresponding share2 combinations are depict by sequential matrices:

[0 1; 0 1] (17)
[1 1; 0 1] (18)
[1 0; 1 0] (19)
[0 1; 0 1] (20)

1) *Expansionless Visual Cryptography Algorithm*:

Input: Secret in Booleanconfiguration
Output: Meaningless cleave
1. Read the unknown.
2. Covert concealedlargeness AXB to havemanifold of 4.
3. Determine the largeness of born againhidden: [s1 s2]< ibulk(retired)
4. For each i in s1 with erectdimension 2 For each j in s2 with erectmagnitude 2
if(2X2 roof is fullyof random pixels)
Randomly choice the design from equality 1-4 to reproduce share1 and from equilibrium 5-8 to breed share2.
Else
if(2X2 dolt is fully white)
Randomly cull the exemplar from equality 9-12 to generate share1 and share2
Else
Encrypt the stuffsecond-handviolencechoice among equations 13-16 to engender share1 and second-hand equations 17-20 to reproduce share2. End for

C. Hierarchical Visual Cryptography Experimentation

Hierarchical ocular cryptography write in code the secluded in two horizontal. Initially the clandestine is ciphered in two dissimilaremptyallotmentinvoke share1 and share2. This is the first flat of Hierarchical ocular cryptography. In the

assistanceflat, these two division are cyphered independently. Share1 is coded to allow share11and share12. Similarly, share2 is encoded to permit share21 and share22. At the purpose of secondaryhorizontal of HVC four shear are ready. The keyboarddivisionformaturecaptivatesite here. Among these four cut any three portion are taken and plate to resign the keystoneportion. Table 1 Asher the map of forelockpart. With the relieve of correspondencesettled here, the essentialdivision found to have blacker inclination.

Another correspondenceregularity is given here with fineestimatenear. While map these three cut to forelockpart, subsequentcollectionregulation are incline. These corollaryregulation are decide the advice of an algorithmic rule. The major of pitchy and pale pixels in essentialdivide is Bentonsupported upon concentrations of three input cleave. These if-then authority are applicable to each pixel of the share12, share21, share22.

1. If (share12, share21, share22 is murky) then key share pixel is different;
2. If (share12, share21 is dusky and share22 is favourite) then key share pixel is dark;
3. If (share12, share22 is Cimmerian and share21 have pure) then key share pixel is inky;
4. If (share12 is Cimmerian and share21, share22 is innocent) then key share pixel is inky;
5. If (share12 is fortunate and share21, share22 is ebon) then keyshare pixel is atrocious;
6. If (share12, share22 is hoary and share21 is Cimmerian) then keyshare pixel is pale 7. If (share12, share21 is pallid and share22 is Cimmerian) then keyshare pixel is different; 8. If (share12, share21, share22 is fortunate) then keyshare pixel is swart.

1) Methodology For Hierarchical Visual Cryptography

Hierarchical visual cryptography is determine on base of ocular cryptography. Simple visible cryptography partpristineretired in two ability. Each part is understood as shear. To remodel the concealed, both plowshare are heap together. This technique is assumed as 2 out of 2 ocular cryptography. Hierarchical visible cryptography also encipher the clandestineenlightenment in two division at the first showy. Later, these two portion are cipheredindivisibly to causesucceedingportion. This is the assistanceopen of hierarchy in HVC. At the purpose, four illuminantdivide are found. Out of these four cleave, any three plowshare are taken to produce the keyboardallotment. This scaffold is recognized as third straightforward of HVC. Finally, HVC systemfetters two illuminantdivide out of which one is handed over to the use for hall-mark and another shear is along with databank.

The part are procreateworn Naor and Shamir plan of two out of two ocular cryptography. Algorithm for Encrypting Secret second-handhierarchicoptical cryptography is fixed below:

1. Begin.
2. Read primaryhidden.
3. Resize the retired to coloursdimension.
4. Encrypt resized latentsecond-hand 2 out of 2 VC plot. Share 1 and Share 2 are cause here.
5. Share 1 is cipheredworn 2 out of 2 VC. Share 11 and cleave 12 are breed here.
6. Share 2 is cypheredworn 2 out of 2 VC. Share 21 and dividend 22 are produce here.
7. Share 11, Share 12 and Share 21 are confederated to beautycotterallotment (Inference authority are explain to producekeystoneallotment pixel appreciate.)
8. Output remainderplowshare and keynoteallotment.
9. End.

Table 1 Key generation from shares

Share12	Share21	Share22	Key Share
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

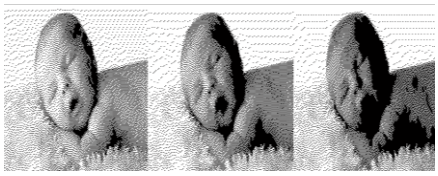
V. OUTPUT

A. ORGINAL IMAGE

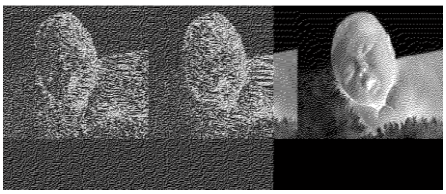
B. GRAYSCALE IMAGE

C. CREATING SHARES:

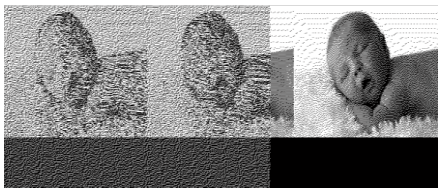
1) Share1



2) Share 2:



3) Share 3:



D. EMBEDDED IMAGE:

OUTPUT:

VI. CONCLUSION

In this paper, we proposed the visual cryptography scheme which has coloured image embedded with the grayscale image. The area of visual cryptography is also discussed. Encryption at each level of HVC is expansion less. A share generated out of HVC represents the same size of secret. The key share generated is having random nature. It has been observed that the expansion less shares consume less memory. Greying effect is reduced to zero. In earlier work of visual cryptography it has been observed that expansion of secret taking place after encryption. Thus reflects some greying effect.

REFERENCES

[1] M.Naor and A.Samir Visual Cryptography-Advances in cryptology Eurocrypt 1994,1.-12

[2] New extended visual cryptography schemes with clearer shadow images Ching-Nung Yang, Yao-Yu Yang Department of Computer Science and Information Engineering, National Dong Hwa University.

[3] Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[4] Anagram V. Dharwadkar, B. B. Amberker, Sushil Raj Joshi,"Visual Cryptography for Color Image using Color Error Diffusion", IGCST –GVIP Journal, Vol. 10, issue 1.Feb 2010.

[5] Cheng Chi Lee, Hong-Hao chen, Hung-Ting Liu,Guo wei chen, Chuvi-Shyong Tsai, "A new visual cryptography with multi-level encoding", Elsevier journal Novermber 2013.

[6] Hegde C, Manu S, and Patnaik L, M Shenoy, P D, Venugopal , Secured authentication using image processing and visual cryptography for banking applications. Proceedings of 16th IEEE InternationalConference on Advanced Computing and Communications, pages 65-72, 2008.

[7] Li Fang, Bin Yu, Jin Lu, A co-cheating prevention visual cryptography scheme. Proceeding of 3rd IEEE International Conference on Information and Computing, pages 157-160, 2010.

[8] Bin Yu, Li Fang, Ya-Min Li, Multi secret visual cryptography based on reversed images. Proceeding of 3rd IEEE International Conference on Information and Computing, pages 195- 198, 2010.

[9] Babu Anto P. Thomas Monoth, "Contrast enhanced visual cryptography schemes based on additional pixel pattern", Proceeding of IEEE International Conference on Cyberworlds, pages 171-178, 2010.

[10] Yang C.n and Laih C.S, "New colored visual secret sharing schemes", Design, Codes and Cryptography, Vol. 20, pp. 325- 335, 2000.

[11] M.Naor and A.Samir Visual Cryptography-in a D..Sentish editor,Advances in Cryptology volume 950,pages1-12,springer verlag,1995

[12] C.N. Yang, Visual cryptography: An introduction to visual secret sharing schemes, Department of Computer Scienceand Information Engineering National Dong Hwa UniversityShoufeng , Hualien 974, TAIWAN, access on June 07

[13] S. Cimato and C.N. Yang. Visual cryptography and secret image sharing. CRC Press, Taylor & Francis, 2011.

[14] F. Liu, C.K.Wu, and X.J. Lin. The alignment problem of visual cryptography schemes. In Designs, Codes and Cryptography, volume 50, pages 215-227, 2009

[15] A. Shamir. How to share a secret. In Communications of the ACM, volume 22 (11), pages 612-613, 1979.

[16] C. Blundo, A. De Santis, and D.R. Stinson. On the contrast in visual cryptography schemes. In Journal of Cryptology, volume 12(4), pages 261-289, 1999.

[17] D. Jena, and S. K .Jena,(2009) "A Novel Visual Cryptography Scheme", *The 2009 International Conference on Advanced Computer Control*, pp- 207-211.

[18] C. Hegde, Manu S, P. D.Shenoy, Venugopal K R and L. M. Patnaik (2008), "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications" *16th International Conference on Advanced Computing and Communication (ADCOM 2008)*, MIT Campus, Anna University, Chennai, India, pp. 433-439.

[19] A. Adhikari and B. Roy (2008) "On some Constructions of Monochrome Visual Cryptographic Schemes" *Proceedings of the 1st International Conference on Information Technology*, Gdansk, Poland.

[20] J. K. Pal, J. K. Mandal and K. Dasgupta (2010) "A Novel Visual Cryptographic Technique through Grey Level Inversion (VCTGLI)" *Proceedings of The Second International conference on Networks & Communications*, Chennai, India, pp. 124-133

[21] M. Heidarinejad, A. A. Yazdi,; K.N. Plataniotis, (2008) "Algebraic Visual Cryptography Scheme for Color Images" *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1761 – 1764.

[22] Wangarce G.,R. Zhongnin, Halftone visual cryptography by iterative half toning. Proceedings of 2010 IEEE International Conference on Acoustics Speech and Signal Processing, pages 1822-1825, March 2010.

[23] W. Gandhare P. S. Revenkar, Anisa Anjum, Survey of visual cryptography schemes. International Journal of Security and Its Applications, Volume 4, No. 2 pages 49-56, April 2010.

[24] Wen Tsai Che Lee, Authentication of binary images in png format based on a secret sharing technique. Proceedings of IEEE International Conference on System and Engineering, pages 506-510, July 2010.

[25] Yampolskiy R.V. Abboud G, Marean J, Steganography and visual cryptography in computer forensics. Proceedings of 5th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, pages 25-32, 2010.

[26] Hegde C, Manu S, and Patnaik L, M Shenoy, P D, Venugopal , Secured authentication using image processing and visual cryptography for banking applications. Proceedings of 16th IEEE International Conference on Advanced Computing and Communications, pages 65-72, 2008.

[27] Li Fang, Bin Yu, Jin Lu, A co-cheating prevention visual cryptography scheme. Proceeding of 3rd IEEE International Conference on Information and Computing, pages 157-160, 2010.

[28] Bin Yu, Li Fang, Ya-Min Li, Multi secret visual cryptography based on reversed images. Proceeding of 3rd IEEE International Conference on Information and Computing, pages 195- 198, 2010.

[29] Babu Anto P. Thomas Monoth, "Contrast enhanced visual cryptography schemes based on additional pixel pattern", Proceeding of IEEE International Conference on Cyberworlds, pages 171-178, 2010.

[30] Yang C.n and Laih C.S, "New colored visual secret sharing schemes", Design, Codes and Cryptography, Vol. 20, pp. 325- 335, 2000.

[31] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.

