International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-100 PAGE NO: 574-579.

SEPARATE DATA EXTRACTION IN ENCRYPTED IMAGES BY REVERSIBLE DATA HIDING USING SIRDS

M. KARTHIK
Research scholar,
Department of Computer Science,
Tamil University, Thanjavur
karthikrj69@gmail.com

K.RAVIKUMAR
Assistant Professor,
Department of Computer Science,
Tamil University, Thanjavur
ravikasi2011@yahoo.com

Abstract**—** Reversible data hiding used to data hidden process in image and also can recover after analyze hidden data in cover image. This RDH schema provides the secrecy of user data’s and also its encoded cover image. Previous methods embedding data in cover(secure) image after retrieving process may be issue is to produced an some errors on data extraction time. most important problem is earlier scheme information hidden in cover image using RDH, hence data retrieval process time were produced an free of errors. In this proposed scheme make SIRDS as secrecy image is share of visual cryptography scheme to reduce transaction risk for both forwarder and receiver like secure information sharing. SIRDS Encoding technique modifies image pixel values using the random dots in the event according to the B-VCS to produce non pixel expansion shares of the B-VCS. Modifying the pixel free dots using a SIRDS will degrade the visual quality of the rebuilder substance. Here, recommend for these model that is based on the visual feature of cover image SIRDS working is based on construction rules for a *(*2, *n)*-B-VCS that maximize the cover image contrast and recovered data strength in the cover image using the B-VCS. SIRDS different type of picture separation after the data bit which was hiding multiple set of pixel, For this the data retrieval method‟ require the index position of those blocks which were considered in hiding process and the pixel pairs position where the data is hidden as the input. The experimental results for our proposed method offers better performance over previous work.

INDEX TERMS:

RDH, Privacy Protection, SIRDS, VCS, Pixel Expansion.

INTRODUCTION

RDH is successful communication technology; desires for information sharing and transfer have increased exponentially. The threat of an eavesdroppers accessing secret information has been an ever existing concern for the information communication in the public region. Steganography and Cryptography are the most widely used techniques to overcome these risks.

Cryptography involves switching a plain text into an unreadable cipher text. Other hand, Steganography embeds message into a cover media and hides its existence. A digital image is considered as the transporter in these techniques. These techniques make some level of security of user information. However, neither of them alone is secure enough for sharing data over an unsecure communication is vulnerable to intruder attacks and channel. Although these techniques are often combined together to complete higher levels of security there still is a need of a highly secured system to share information over any communication media minimizing the risk of intrusion.

Visual cryptography is a powerful technique that merges the notions of ciphers and secures sharing in cryptography with that of graphics. VC takes a binary data and divides it into two or more section known as shares. When the shares are written on transparencies and then superimposed, the secret data can be recovered well again. Visual cryptography is a unique technique in the logic that the encrypted message can be decrypted directly by the (HVS). It focuses on resolving the problem of secret sharing. A secure sharing method suggested by Shamir’s and Naor [2] enables allocation of a secret amongst *n* parties, such that only predefined unauthorized sets will be able to reconstruct the secret information. In a *k* out of *n* secret data sharing problem *n* transparencies are produced and it needs a smallest amount

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-100 PAGE NO: 574-579.

of *k* shares to retrieve well again the original image (message). The image remains hidden if fewer than *k* transparencies are stacked mutually. Each and every pixel appears within *k* modified versions known as shares. The shares are a group of *m* black and white sub-pixels arranged closely together.

Before the development of digital means, conventional methods were creature used for transferring or receiving messages. Before mail messages, before phones were sent on end. For the messages where privacy was of prime concern, the behavior of implementing protection were following:

- Write the information using such notations that actual meaning of the message was concealed.
- choose the messenger skilled of delivering the information securely.
- secrete the communication such that even its presence can't be predicted.

In steganography, the possible cover carriers are innocent looking (text, audio, video, and images) which will hold the hidden data. A message is the information hidden and may be cipher text, plaintext, images, or anything else that can be embedded into a bit stream (binary data). The cover carrier and the embedded message create a stego-image (carrier). Embedding data may need stego key which is additional secret data, such as a password, required for hiding the secure information. Example, when secret information is embedding within a cover image, the resulting product is a stego-image like cover image.

A possible formula may be represented as:

Cover medium + embedded message + stego key = stego-medium

DEFINITION :

femd : steganographic function "embedding"
fext : steganographic function "extracting"
Cover: envelop data in which *emb* will be secreted
Embed: message to be hidden stegno: cover data with the hidden message

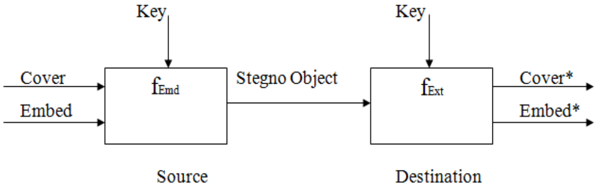


Fig 1 the Steganographic System

The benefit of steganography is that can be used to secretly transmit data's without the reality of the transmission being discovered. Often, using encryption might recognize the receiver or sender as somebody with something to hide.

Reversible data hiding (RDH) in images is a technique, by the original cover can be losslessly recovered after the embedded message be extracted. This important method is widely used in medical descriptions, military imagery and law forensics, where no distortion of the unique cover is acceptable

VISUAL cryptography is a technique that encrypts a secure data into *n* shares, with each applicant holding one share on secure image; any applicant with fewer than *k*, $2 \leq k \leq n$, shares cannot reveal any information about the top secret image. Stacking the *k* shares reveals the underground image, which can be acknowledged directly by the human visual system [4]. Conventional shares [3]–[1], which consist of many random and meaningless pixels satisfy the security requirement for protecting secret contents, but they have a drawback—there is a high transmission risk because noise-like shares raise the suspicion of attackers, who may intercept the shares. Thus the risk both to the participants and to the shares increases in turn increasing the probability of transmission failure.

PREVIOUS ARTS

All previous techniques hided data by reversibly vacating room from the embedded images, which may be issue to some errors on data retrieval and image restoration.

In a data owner encrypts the original image using a regular cipher text with a secret key. Then producing encrypted image, the data owner hands over it to a data hider and the data hider can embed some auxiliary information into the encrypted image by lossless vacating some room according to a data hiding key. Then a receiver, maybe the data owner himself or an authorized third party can extract the embedded secure data with the data hiding key and further recover the original image(data) from the encrypted version according to the encryption key.

In all techniques of the encrypted 8 bit gray-scale images are generated by encrypting every bit - planes with a stream cipher. The method in fragments the encrypted image into a number of non overlapping blocks sized by each block is used to carry one added bit. The method fragments the encrypted image into a number of non overlapping blocks sized by a * a each block is used to carry one added bit.

To do this, pixels in each block are pseudo-randomly separated into two sets S1 and S2 according to a secure data key. If the extra bit to be embedded is 0, flip the 3 of each encrypted pixel in S1, otherwise flip the 3 encrypted of pixels in S2. data extraction and image recovery, the receiver flips all the three pixels in S1 to form a new decrypted block, and flips all the three pixels in S2 to form another new block; one of them will be decrypted to the original block. Due to spatial relationship in natural images, original block is presumed to be smoother than hindered block and embedded bit can be retrieval correspondingly. There is a threat of defeat of bit extraction and image recovery when divided block is relatively small or has much fine-detailed textures.

Hong [11] reduced the error rate of Zhang's method [16] the pixels in calculating the smoothness of all block and using plane match. The recovery and extraction of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate the smoothness of unrecovered blocks, which is referred to as plane match.

Zhang's method in [12] pseudo-randomly permuted and divided encrypted image into a number of groups with size of L. The LSB-planes of each one group are compressed with a parity-check matrix and the vacated room is used to embed data. At the receiver side, the 8-P most significant bits (MSB) of pixels are obtained by decryption directly.

PROPOSED METHOD:

Julesz implemented the random-dot format of the stereogram, in which the 3D form find a way around the monocular processes and is visible only when stereoscopic fusion is obtained. A random-dot stereogram (RDS) is a stereo couple of images of random dots, which when viewed with the support of a stereoscope or with the eyes focused on a point in front of behind the images; generate an awareness of depth, with objects appearing to be in front of or behind the display level. Clarke and Tyler proposed a stereoscopic technique that allows the stereoscopic presentation of 3D form from a single printed image by a random dot pattern. That method is known as Random Dot Auto stereograms or Single Image Random Dot Stereogram's (SIRDS).

The emergence of a SIRDS consists of numerous random dots that have a similar appearance with shares in a Visual Cryptography System. The only difference is that people can reconstruct the original object via binocular disparity from a SIRDS. Hence, hiding a share of a VCS in a SIRDS can decrease suspicion of hidden secrets. The property indicates that the SIRDS is best, and an ordinary, candidate to serve as a cover image for a share of a conventional Visual Cryptography System. This thesis is willing in to developing a technique for sharing visual secrets using SIRDSs.

In the SIRDS, the image contains many random-dot patterns that periodically replicate in the horizontal direction; the stereopsis of the objects arises from differences in the horizontal positions of the image. The pixel allotment in *n* SIRDSs that were generated independently. Suppose each SIRDS has the same pixel density *d*, the probability of pixel distribution pattern.

The pixel distribution connecting all SIRDSs are stacked, each all pixel distribution prototype will uniformly appear in the stacked image. It is approximately impossible to make public any meaningful information by stacking two shares together. Try to modify any pixels in SIRDSs such that the modified SIRDSs can share secret Information (images) the same way as VCSs. In the following, will inspect whether the modified pixels in a SIRDS will interfere with the visual effect of stereopsis in the SIRDS.

This observation indicates that the altered SIRDSs can be detected by a human visual system, thus making it difficult to share extra information in RDS. Hence, there are a transaction between keeping the visual quality of stereopsis in a SIRDS and producing a high-quality VCS. When try to construct a specific VCS from a set of SIRDSs, it may be necessary to alter a large number of random pixels to observe the pixel distribution regulation of the VCS. However, these altered pixels can be perceived as an illusion of 3D depth and these interfere with the original stereopsis in the SIRDS. On the above observation, formulated a mathematical optimization model to discover an most favorable solution to share a secret image in SIRDSs where the objective is to maximize contrast under the restriction of the visual quality of SIRDSs. Using this model, dealers can adjust the visual quality of SIRDSs to obtain the best display quality of the recovered images.

This implementation propose a *(*2, *k)*-BVCS for sharing a binary secret image in *n* SIRDSs. The proposed encryption process is shown in Fig. 2. The first phase, *n* depth maps are used to produce *n* SIRDSs using the auto stereogram generator. In the proposed *(2,k)*-BVCS, each depth map has the same image size and all generated SIRDSs have the same pixel density *d*.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

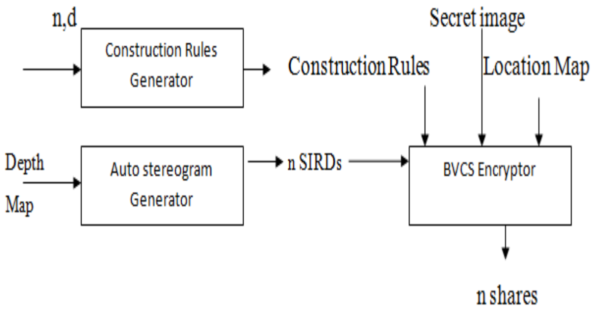


Fig 2 two-phase encryption process of *(k, n)*-BVCS.

The construction rules generator, based on given parameters, *n* and *d*, of each SIRDS, generates guidelines for altering pixels in the SIRDSs. The encryptor alters pixels only within a specific region, which is called the encryption region, where black secret pixels appear. Due to the altered pixels could be disclosed in the verification image of a SIRDS. To preserve the security condition for each share of the BVCS, the encryption region will be enlarged to cover neighbors of the black secret pixels. The construction rules of a BVCS consist of two *(n* + 1) × *(n* + 1*)* matrices, M0 and M1, for sharing white and black secret pixels in a secret image.

Next, design an encryption algorithm for the BVCS encryptor. Based on the modification rule for a given BVCS, the algorithm alters pixels on *n* SIRDSs, ST1,. . ., ST*n* , to share a binary secret SE.

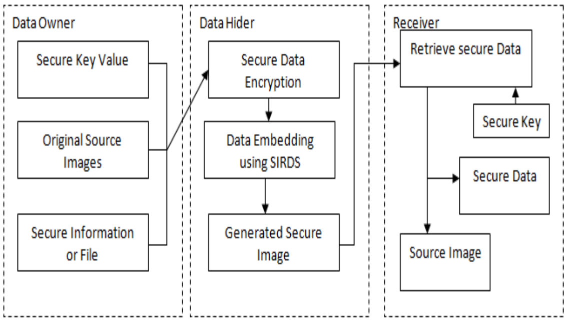
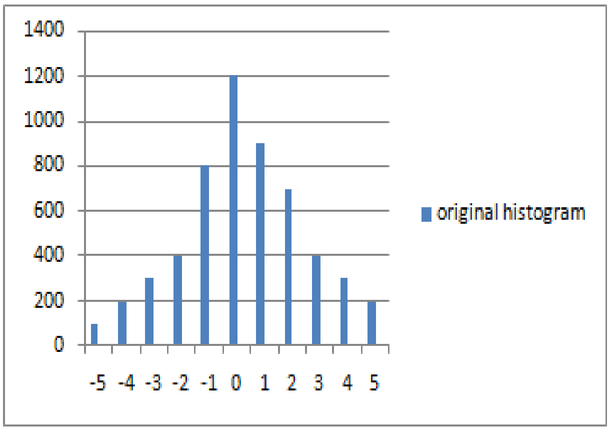


Fig 3 Architecture Diagrams

EXPERIMENTS AND COMPARISONS:

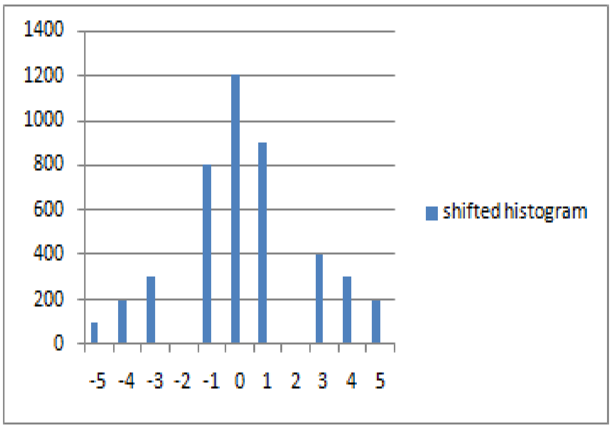
In this section, discuss an experiments that conducted to evaluate the presentation of the development new method (2, *k)*-BVCSs. also there present some demonstrations of the execution results for observing the visual effects of the BVCSs. Finally, compare the properties of this study with previous approaches.

Histogram Comparison



Original histogram

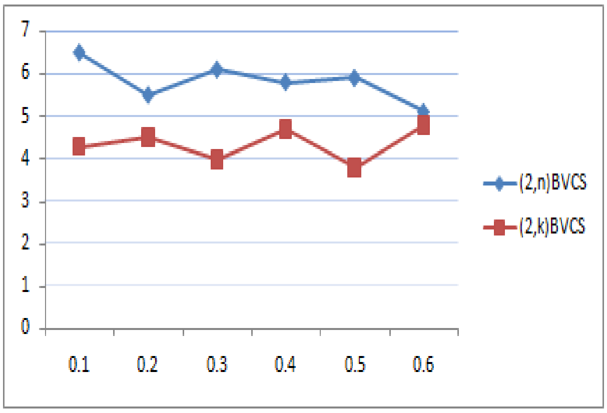
The calculate approximately error is estimate via some data can be embedded into the estimating error sequence with histogram shift.



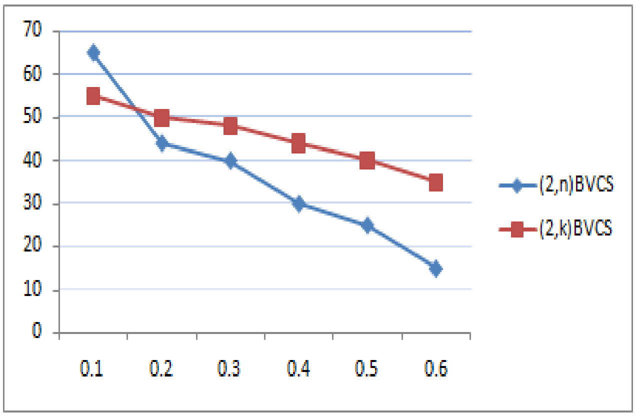
Shifted histogram

The development can be as high as 2 to 4 dB at low embedding rate. As for quality images such as Baboon with rather flat error histogram, the second solution has a better performance of 1 to 2 dB.

Encoding and Decoding Time Comparison



Encoding Time Comparison



Encoding Rate

CONCLUSION:

SIRDS is a new method drawing attention because of the privacy requirements from public environment information management. Earlier method implement RDH in encrypted images by vacating room after encryption, which proposed by reserving room before encryption. This thesis work proposed a *(*k, *n)*-BVCS and developed a new technique for hiding a size-invariant in *n* SIRDSs. This work explored the possibility of hiding a share of a VCS in SIRDS that are printed on transparencies. The greatest recovered images in *(*k, *n)*-B-VCS, 2 ≤ *n* ≤ 10, ranges and SIRDs can produce clear recovered images for a (k, *n)*-B-VCS. The experimental results establish the effectiveness and the flexibility of the proposed *(*k, *n)*-BVCS efficient encoding rate and processing time little bit is increased. In the future work secure information will be encrypt then embedding into the secret image like second time verification, that encryption algorithm like AES, Blowfish and RSA etc.

REFERENCES:

[1] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, “Image size invariant visual cryptography,” IEICE Trans. Fundam. Electron., Commun., Comput. Sci., vol. E82-A, no. 10, pp. 481–494, 1999.

[3] C. N. Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, Mar. 2004.

[4] P. L. Chiu and K. H. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[5] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no 8, pp. 890–896, Aug. 2003.

[6] Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[7] D.M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007.

[8] X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol. 89, pp. 1129–1143, 2009.

[10] L. Luo et al., “Reversible imagewatermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

[13] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[15] T. Guo, F. Liu, and C. Wu, "k out of k extended visual cryptography scheme by random grids," Signal Process., vol. 94, pp. 90–101, Jan. 2014.

[16] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453,
Aug. 2006.

[17] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[18] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[19] H. W. Thimbleby, S. Inglis, and I. H. Witten, "Displaying 3D images: Algorithms for single-image random-dot stereograms," *Computer*, vol. 27, no. 10, pp. 38–48, Oct. 1994.

[20] W. Zhou and A. C. Bovik, "A universal image quality index," *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, Mar. 2002.