ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SIRDSS: Sharing Secret Images via high Quality Shares with Significant Visual Information



Izzath Unnisa Begum
Student,
Department of CS,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Ms.Medapati Lalitha
Associate Professor,
Department of CSE,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Khadarbi Shaik
HOD,
Department of CS,
Shadan Women's College of Engineering & Technology,
Khairatabad, Hyderabad.

Abstract:

Visual cryptography schemes (VCSs) generate random and meaningless shares to share and protect secret images. Conventional VCSs suffer from a transmission risk problem because the noise-like shares will raise the suspicion of attackers and the attackers might intercept the transmission.

Previous research has involved in hiding shared content in halftone shares to reduce these risks, but this method exacerbates the pixel expansion problem and visual quality degradation problem for recovered images.

In this paper, a binocular VCS (BVCS), called the (2,n)-BVCS, and an encryption algorithm are proposed to hide the shared pixels in the single image random dot stereograms (SIRDSs). Because the SIRDSs have the same 2D appearance as the conventional shares of a VCS, this paper tries to use SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares.

The encryption algorithm alters the random dots in the SIRDSs according to the construction rule of the (2, n)-BVCS to produce nonpixel-expansion shares of the BVCS. Altering the dots in a SIRDS will degrade the visual quality of the reconstructed 3D objects. Hence, we propose an optimization model that is based on the visual quality requirement of SIRDSs to develop construction rules for a (2, n)-BVCS that maximize the contrast of the recovered image in the BVCS.

INTRODUCTION

What Is Image Processing?

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. It is among rapidly growing technologies today, with its applications in various aspects of a business. Image Processing forms core research area within engineering and computer science disciplines too.

Image processing basically includes the following three steps:

Importing the image with optical scanner or by digital photography.
Analyzing and manipulating the image which includes data compression and image enhancement and spotting patterns that are not to human eyes like satellite photographs.
Output is the last stage in which result can be altered image or report that is based on image analysis.

Purpose of Image processing:

The purpose of image processing is divided into 5 groups. They are:

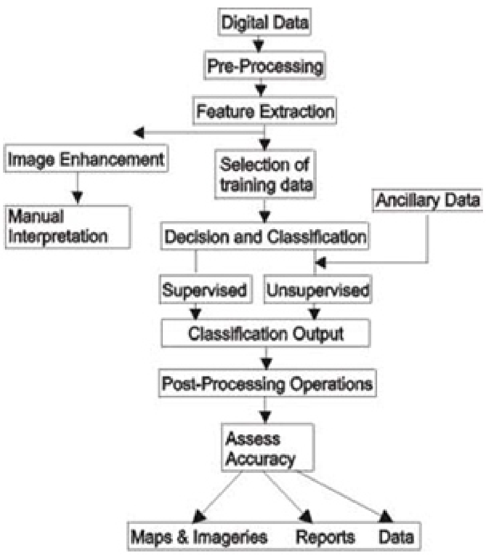
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1.Visualization - Observe the objects that are not visible.
2.Image sharpening and restoration - To create a better image
3.Image retrieval - Seek for the image of interest.
4.Measurement of pattern – Measures various objects in an image.
5.Image Recognition – Distinguish the objects in an image.

Types of Image Processing:

The two types of methods used for Image Processing are Analog and Digital Image Processing. Analog or visual techniques of image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. The image processing is not just confined to area that has to be studied but on knowledge of analyst. Association is another important tool in image processing through visual techniques. So analysts apply a combination of personal knowledge and collateral data to image processing. Digital Processing techniques help in manipulation of the digital images by using computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of processing. The three general phases that all types of data have to undergo while using digital technique are Pre- processing, enhancement and display, information extraction.

Working diagram of Image Processing:



Characteristics of Image Processing:

Before going to processing an image, it is converted into a digital form. Digitization includes sampling of image and quantization of sampled values. After converting the image into bit information, processing is performed. This processing technique may be, Image enhancement, Image restoration, and Image compression.

Image enhancement:

It refers to accentuation, or sharpening, of image features such as boundaries, or contrast to make a graphic display more useful for display & analysis. This process does not increase the inherent information content in data. It includes gray level & contrast manipulation, noise reduction, edge crispening and sharpening, filtering, interpolation and magnification, pseudo coloring, and so on.

Image compression:

It is concerned with minimizing the number of bits required to represent an image. Application of compression are in broadcast TV, remote sensing via satellite, military communication via aircraft, radar, teleconferencing, facsimile transmission, for educational & business documents, medical images that arise in computer tomography, magnetic resonance imaging and digital radiology, motion, pictures, satellite images, weather maps, geological surveys and so on.

- Text compression – CCITT GROUP3 & GROUP4
- Still image compression – JPEG
- Video image compression – MPEG

Advantages of Image Processing:

- The processing of images is faster and more cost-effective. One needs less time for processing, as well as less film and other photographing equipment.
- It is more ecological to process images. No processing or fixing chemicals are needed to take and process digital images. However, printing inks are essential when printing digital images.
- When shooting a digital image, one can immediately see if the image is good or not.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

• Copying a digital image is easy, and the quality of the image stays good unless it is compressed. For instance, saving an image as jpg format compresses the image. By resaving the image as jpg format, the compressed image will be recompressed, and the quality of the image will get worse with every saving.
• Fixing and retouching of images has become easier. In new Photoshop 7, it is possible to smoother face wrinkles with a new Healing Brush Tool in a couple of seconds.
• The expensive reproduction (compared with rastering the image with a repro camera) is faster and cheaper.
• By changing the image format and resolution, the image can be used in a number of media.

EXISTING SYSTEM:

The cryptographic approach uses a set of basis matrices or an algorithm to simultaneously encrypt a VCS and provide a meaningful appearance for the shares of the VCS. The former method requires designing a set of basis matrices for a specific VCS, and suffers from the pixel expansion problem. The random-grid-based (RG-based) approach (an algorithmic method) involves constructing VCSs and EVCSs. The main idea behind the RG-based EVCS algorithm approach is that it encrypts a secret image to the shares according to a given probability p and stamps cover images on the shares with (1−p) probability.

The encryptions of the secret image can use any existing RG-based VCS. By adjusting probability p, the algorithm can tune the visual qualities between the recovered image and the shares of an EVCS. Chen et al. and Guo et al. proposed RG-based (2,2)-and(k,k)-EVCSs, respectively. Chen et al.'s approach must use a pair of complementary images as cover images. Guo et al.'s approach does not need to adopt complementary images as cover images, but the visual quality of the shares is reduced when probability p is too small or too large.

Draw backs:

Although both SIRDSs and shares of VCSs have the same noise-like appearance, the pixel distributions for a set of SIRDSs and for shares of a specific VCS are quite different.

The pixel distribution among shared pixels must obey the construction rules or codebooks of the VCS. Shared pixels mean that a set of pixels shares the same secret pixel in a VCS.On the other hand, in a SIRDS, the image contains many random-dot patterns that periodically repeat in the horizontal direction; the stereopsis of the objects arises from differences in the horizontal positions of the image. The pixel distribution in n SIRDSs that were generated independently is totally independent.

PROPOSED SYSTEM:

A 2-out-of-n binocular VCS, called the (2, n)-BVCS, is proposed to provide non-expanded and high-quality cover images for shares of the VCS to reduce the risk of interception during the transmission phase. The proposed (2, n)-BVCS shares a binary secret image with n participants (n≥2); when any two participants stack their transparences, the encrypted secret is revealed. The shares of the (2, n)-BVCS are hidden in n SIRDSs to reduce susceptibility to attackers during the transmission phase. The proposed encryption procedure consists of two phases. In the first phase, the procedure generates n SIRDSs by using existing auto stereogram generation programs. In the second phase, the procedure alters the random dots in the SIRDSs according to a construction rule of the (2, n)-BVCS for hiding the binary secret image. The construction rule is a guideline for hiding the secret image in the SIRDSs securely.

ADVANTAGES:

Altering the dots in a SIRDS will interfere with the human brain's ability to perceive the original 3D objects in the SIRDSs and degrade the visual quality of the reconstructed 3D objects. Hence, we adopt an optimization approach to find construction rules for the (2, n)-BVCS such that the encryption process yields a secure BVCS and the contrast of the recovered secret image can be maximized, subject to the visual quality of the SIRDSs.

IMPLEMENTATION:

Two-Phase Encryption:

We propose a(2,n)-BVCS for sharing a binary secret image in n SIRDSs. The proposed two-phase encryption process is shown.In the first phase, n depth maps are used to produce n SIRDSs using the auto-stereogram

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

generator that adopts Thimble by's algorithm. In the proposed (2, n)-BVCS, each depth map has the same image size and all generated SIRDSs have the same pixel density d. In the second phase, according to construction rules for (2, n)-BVCS, pixels in the n generated SIRDSs are altered to share a binary secret image for the SIRDSs by the (2,n)-BVCS encryptor. Based on the above-mentioned observation, the encryptor tries to reduce the number of altered pixels in a SIRDS to minimize the amount of interference introduced into the resultant share. 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. Hence, a location map, which is a binary image as shown, is used to indicate the encryption regions (i.e., the black regions in the map) for the secret image in the BVCS. At the end of the second phase, n image-size-invariant shares are generated for the(2,n)-BVCS

A. The Basic Idea of the (2, n)-BVCS Construction: The construction rules generator generates construction rules based on pixel density d of SIRDSs and a given access structure of the BVCS. The rules are used to construct the BVCS by altering pixels in the SIRDSs; therefore, the construction rules simultaneously satisfy the conditions of the VCSs and cannot disclose any information related to the secret image in the verification image of a SIRDS.

B. Optimization Model of the (2, n)-BVCS: The (2, n)-BVCS problem is formulated here as an optimization model. Both constants d and n are given and we determine modification matrices M0 and M1for hiding white and black secret pixels in n SIRDSs. The objectives of this problem are to maximize the contrast of recovered secret images and to minimize the alteration probability of each SIRDS under the visual quality and security constraints. The first objective of the proposed model is to maximize the contrast of the recovered image in the (2,n)-BVCS. The contrast value is the most important performance metric in VCSs; hence it is the major objective of the model. The other objective of this model is to minimize the introduced interference for the SIRDSs; hence the model minimizes the alteration probability of each SIRDS. The second objective is related to the visual quality of the SIRDSs. Constraints (C1)–(C3) are the security condition of the (2,n)-BVCS. Constraint (C4) is the visual quality constraint that limits the maximum alteration probability for each SIRDS (share) so that it is no more than Pa,max. By tuning Pa,max, interference in the stereopsis in each SIRDS can be maintained at an acceptable level. Constraints (C5) and (C6) limit the overall modification probability of each pixel distribution pattern for sharing white and black secret pixels, respectively.

The (2,n)-BVCS Encryptor:

Next, we 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,...,STn, to share a binary secret SE. The main idea of the encryption algorithm is as follows. Notation Cx,y =[pST1x,y ... pSTnx,y] denotes a collection of pixel colors for nSIRDSs ST1,...,STn at coordinate(x, y). Notation H(Cx,y)denotes the Hamming weight of Cx,y. If pixel pLx,yon location map L is a white pixel (i.e., pLx,y =0),pixelspS1x,y, ..., pSnx,y on the resultantshares S1,...,Sn are the same as pixels pST1x,y,..., pSTnx,y onSIRDSs ST1,...,STn, respectively. Otherwise, resultant pixelspS1x,y,..., pSnx,y could be different from pixels pST1x,y,..., pSTnx,y according to secret image SE andthe modification rules. When the color of secret pixel pSEx,yis white (i.e., pSEx,y =0),theencryption algorithm uses modification rule m0H(Cx,y),0, ...,m0H(Cx,y),nto alter the colors of pixels pST1x,y,..., pSTnx,y toyield resultant pixels pS1x,y, ...,pSnx,y. On the contrary, theencryption algorithm uses modification rule m1H(Cx,y),0, ...,m1H(Cx,y),nto yield resultant pixels pS1x,y, ..., pSnx,y. Eventu-ally, the distribution of the resultant pixels, iB(n–i)W,will be altered to jB(n – j) W, wherei=H(Cx,y)and 0≤j ≤n.

CONCLUSION:

This study proposed a (2, n)-BVCS and developed a new method for hiding a size-invariant (2, n)-VCS in n SIRDSs. This work explored the possibility of hiding a share of a VCS in SIRDSs that are printed on transparencies.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We developed a mathematical model that defines a set of construction rules so that the recovered images of (2, n)-BVCSs have the highest contrast under the constraint of the interference introduced into the SIRDSs. Using this mathematical model, a desired visual quality for shares and recovered images can be found by adjusting parameters Pa,max and d. The best contrast for the recovered images in (2, n)-BVCSs, $2 \le n \le 10$, ranges between 0.5 and 0.2, and can produce clear recovered images for a (2, n)-BVCS. The experimental results prove the effectiveness and the flexibility of the proposed (2, n)-BVCSs. In the near future, we plan to extend this study to explore new methods for hiding a (k, n)-VCS in n SIRDSs.

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] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[6] D. Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," Pattern Recognit., vol. 42, no. 11, pp. 3071–3082, Nov. 2009.

[7] T.-H. Chen and K.-H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

[8] K.-H. Lee and P.-L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

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

Author's:

Ms.Izzath Unnisa Begum has completed her B.Tech. in Information Technology from Nawab shah Alam Khan Of College of Engineering and Technology, JNTU University , Hyderabad. Presently, she is pursuing her Masters in Computer Science from Shadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, T.S, India. Her research interests include image processing, and data mining.

Ms.Medapati Lalitha has completed her M.SC (Information technology) from Allagappa university and M.tech(CSE) from Nagarjuna University. She has 11 years working experience in teaching field. Currently working as an Assistant professor of CSE Department in Shadan Women's College of engineering and technology, Hyderabad, T.S. India .

Ms.Khadarbi Shaik has completed her B.tech(CSE) from Andhra University and M.tech(CSE) from SRM University. She has 6 years working experience in teaching field. Currently working as an Assistant professor and H.O.D of CS Department since 2 years in Shadan Women's College of engineering and technology, Hyderabad, T.S. India