ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (301-304), Month: January - March 2016, Available at: www.researchpublish.com

SHARING SINGLE IMAGE USING VISUAL CRYPTOGRAPHY

[1]Minu Antony, [2]Neethu Mol Abraham, [3]Ushus Maria Joseph

[1]IV Year, B.Tech Student Dept of CSE, MBCCET, Peermade 686513, idukki, kerala,india
[2]IV Year, B.Tech Student Dept of CSE, MBCCET, Peermade 686513, idukki, kerala, india
[3]Assistant Professor, Dept. of CSE, MBCCET, Peermade686513, idukki, kerala, india

Abstract: **Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. In this paper (2,n) BVCS and an encryption algorithm are proposed to hide the text, audio and image that should be fed as a digital image in the system as the input and the system generates "n" (2≤n) numbers of different images called shares, look like images of random noise. Among "n" number of shares user has to stack "k" number of shares, where 2≤k≤n, to reveal the secret. In order to reduce the transmission risk of the shares, SIRDSs are used as cover images of the shares of VCSs. The audio recorded is converted to text and is encrypted using an image. It is then send to the receiver, who decrypts the encrypted data and the audio and text is revealed.**

Keywords: **Shares, BVCS, Visual cryptography.**

I. INTRODUCTION

Visual Cryptography is an encryption method that encrypts information such as(secret image, audio and text) which is divided into n shares , any person with less than k shares, 2≤ k ≤ n, shares do not convey any information about the hidden content. Stacking k shares convey the hidden information, that can be directly recognized by human visual system[1].Ordinary shares[1]-[4], that consist of many disordered and pixels that will not have any sense satisfy the security requirements for protecting the hidden contents, but they have a major disadvantage, there is a high transmission risk and the attackers can intercept the shares.

Thus the unfavorable condition both to the person and to the shares increments which in turn increments the chance of transmission failure In earlier examination into the Extended Visual Cryptography Scheme [EVCS] provides a significant appearance for shares in order to make commotion like shares manageable for persons.

In EVCSs, each shares is printed on separate transparencies contain many commotion like pixel and display low quality information such shares sensible for members. Zhou et al. proposed a (2, 2)- VCS utilizing the half conditioning system to develop important paired pictures as shares conveying significant visual data [10].The visual quality of half conditioning is better than extended VC. Zhouet a.l's process can lessen the transmission danger of the shares Other researches also suffer the same disadvantage as that of Zhoueta.l's process.

In 1838, Wheatstone developed stereoscopic vision and distributed a clarification of stereopsis emerging from contrast in the level position of pictures in the two eyes. An irregular dab stereogram is a stereo pair of pictures of arbitrary dots, which when seen with the guide with the stereoscope or with the eyes concentrated on a point before or behind the picture deliver's an impression of profundity, with the article having all the earmarks of being before or behind the showcase level. Tyler and Clarke proposed a stereoscopic presentation of 3D structure from a solitary printed picture by an irregular spot design. This method is also known as Single Image Random Dot Stereogram's otherwise is known as Random Dot Auto stereograms. The SIRDS consist of many random dots that have a similar to the share in a VCS. The main difference is that person can recreate the original 3D entity by means of binocular different from a SIRDS.

In this paper, an encryption algorithm is proposed to provide shares that are not expanded and also provides high definition and quality cover images to reduce the unfavorable condition during the transmission phase. By this algorithm,

a binary secret information is divided into n shares, where each shares is printed on separate transparencies and stacking each shares can reveal the secret information. The audio composed is concerted to text an encrypted by using cover image and transmitted the receiver receive it the encrypted data is then decrypted, those the audio and text can retrieved.

II. RELATED WORK

The VCSs can be classified into two methodologies, cryptography approach and embedded approach. The cryptography approach are generally used in premise grid [5],[6] or algorithm [7],[9] to encrypt a VCS and provide important appearance for the shares of VCS. The previous method outlining arrangement of set of premise grid for a specific VCS, and issues from the pixel expansion problem The random-grid based method includes developing VCSs and EVCSs [7],[9]. The main concept of RG based EVCS algorithm method is that it encrypt a secret information to the shares according to a give likelihood p and stamp cover image on the shares with (1-p) likelihood. The encryption of the secret information can any current RG based VCS. By utilize likelihood p, the calculation can adjust the visual important between the recovered information and the of an EVCS. Chen et al. and Gueo et al. proposed RG based (2,2) and (k,k) EVCSs. Chen et al method must utilize a couple of complementary picture as spread images. Guo et al proposed method does not have chosen complementary picture as spread images. But in this case visual quality is decreased when likelihood p is too little or too expensive. Zhou et al develop a halftone VCS that can proposed (2,2) EVCS s by means of reciprocal of spread shares [10]. To start with, they prepared a couple of complementary halftone image.

Zhou's approach the measure of halftone cell must be greater than or equivalent to the pixel expansion factor. The visual important of the halftone shares enhance the measures of a halftone increment. On the other hand there is an exchange between the visual important of shares and the visual nature of the spread images. Zhou's method can be proposed to an arbitrary access structure but this case provides many several image to distribute person. The proposed method can be divided into embedded approach. There are two main differences between this study and the past examination. First place, this study receive SIRDSs as spread image of VCSs. Second places, this study show new developing rules for sharing secret information as opposed to utilize the traditional premise grid or RG based calculation.

III. IMPLEMENTATION

A 2 Out-of-n binocular VCS, called the (2,n)-BVCS, provides good quality images which are not expanded and are divided into n shares that are displayed on each transparencies in order to decrease the transmission risk of these shares. This proposed scheme shares binary secret image with n participants with n greater than or equal to two, when at least any two of the participants stack their transparencies the encrypted secret is revealed. The shares of this are hidden in n SIRDSs to decrease the chances of attack during transmission phase. A SIRDSs is a set of displayed dots that form a 3D view when focused at infinity. Instead of dots, sometimes text characters are also been used.

The (2,n)-BVCS scheme has the following phases such as:

A. Two-phase encryption scheme:

In this phase we propose a (2,n)-BVCS for transferring a binary secret image in n SIRDSs. During the first phase ,n depth maps are used to generate n SIRDSs by using the Auto stereogram generator. An auto stereogram is a single-image stereogram, designed to create a visualization of a 3D scene from a two-dimensional image.

Each n depth maps have similar image size and all the generated SIRDSs has the same pixel density. In the second phase, by the (2,n)-BVCS encryptor pixels in the n generated SIRDSs are changed to transfer binary secret image. The main aim of the encryptor is that it reduces the number of altered pixels in the SIRDSs. The encryptor changes the pixels only within a specified area, where black secret pixels appear are called as encryption region. Each shares of the BVCS is preserved by enlarging the encryption area to cover neighbors of black secret pixels.

B. Construction rule generator:

1. A (2,n)-BVCS construction

The construction rule generator produces construction rules based on the structure of the BVCS and also the pixel density d of SIRDSs. By changing the pixels in the SIRDSs we can develop the BVCS, therefore the construction rules fulfill the condition of VCSs and it do not reveal any information about the secret image. The construction rule consists of two matrices (n+1)*((n+1), M^0 $_{\text{and}}$ M^1 $_{\text{for}}$ transferring black and white pixels in a secret image.

2. Optimization model for (2,n) - BVCS

In this optimization model constants d and n are given and we determine modification matrices m0 and m1 in order to hide white and black pixels in SIRDSs. There are two objectives for this problem ie, to maximize recovered secret image and also to minimize alternation probability under visual quality and security constraints. The first objective of this model is that it maximize the recovered image in (2,n)-BVCSs. The second objective is that it reduces the interference in the SIRDSs, hence it minimizes the alternation probability of SIRDSs.

C. The (2,n)-BVCS encryptor:

The encryption algorithm changes the pixels in n SIRDS, ST1……..STn in order to share the binary secret. The input image includes one secret image and one location map. The output images are n resultant shares S1 to Sn.

Encryption Algorithm:

1. Pixel ElementIndex++;

2. Let state=State.Filling_With_Zeros

3. Increment the value of zeros until it is 8

4. Otherwise return bmp

5. Extract text as bitmap bmp

6. Initialize color unit index and char value

7. Let the extracted text be string extracted Text = String. Empty;

8. Let the I value be greater than bmp.height

9. Let the j value be greater than bmp.width

10. Color the pixel using I and j value

11. Switch (color UnitIndex % 3)

a. case 0:charValue = char Value * 2 + pixel’s % 2;

b. case 1:charValue = char Value * 2 + pixel.G % 2;

c. case 2:charValue = char value * 2 + pixel.B % 2;

12. ColorUnitIndex++;

13. If (colorUnitIndex % 8 == 0), reverse the bits of charvalue

14. If (charValue == 0) then return extracted Text;

15. Convert the character value from int to char

16. Add the current character to the result text then return extracted Text;

17. Compute the result as result=result *2+n%2

18. Return result

19. Stop

IV. CONCLUSION

This model proposes a (2,n)-BVCS where the size invariant (2,n) VCS is hidden in n SIRDs. It developed the possibility of hiding the shares on SIRDSs that are displayed on separate transparencies. Hence the noise-like shares are manageable and visual quality and non-expanded images are produced.

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 and 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

[5] Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

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

[7] 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.

[8] 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.