Proceedings of National Conference on Recent Advances in Computer Science & Engineering (NCRACSE-2017)

International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 01, February 2017
ISSN: 2455-3778
http://www.ijmtst.com

An Advance Privacy Sharing Using Arbitrary Visual Privacy Distributing

G K Kishore Babu[1] | V.Alekhya[2] | L.Srikavya[2]

[1,2,3]Department of CSE, Chalapathi Institute of Engineering & Technology, Guntur, India

To Cite this Article
G K Kishore Babu, V.Alekhya and L.Srikavya, "An Advance Privacy Sharing Using Arbitrary Visual Privacy Distributing", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 01, 2017, pp. 36-39.

ABSTRACT

Visual privacy distributing is the technique that divide theprivacy image into n multiple shares. Each share constitutes some information and when k shares out of n stack together the privacy will reveal. However; less than k shares are not work. Distributing is the idea from privacy distributing scheme that was presented in 1975 by Adi Shamir. The beauty of the Visible Privacy Distributing scheme is its decryption process i.e. to decrypt the privacy using Human Visual System (HVS) without any computation. Visual cryptography is presented by Noar and Shamir in 1995 including also visual privacy distributing. The resultant privacy recover through this scheme is double in size of the original privacy [17]. We have proposed the new algorithms for the (2, 2) visual cryptography and (3, 3) visual privacy distributing. Our proposed schemes are for gray scale image and by stacking the shares; the resultant image achieved in same size with original privacy image and Its shadow Image. We used randomization and pixel reversal approach in all methods.

KEYWORDS: *Privacy distributing, Cryptography , pixel reversal.*

I. Introduction

The concept of privacy distributing was developed many years back, when Adi Shamir has shown this idea in his paper in 1979 [1]. In this paper he shows that" How to divide data into n pieces in such a way that data is simply reformation from any k pieces, but even overall knowledge of k - 1 pieces opens simple no information about data". He utilized this idea to recover the key for using the encryption. In 1994, Naor& Shamir shows a new concept using images in their paper"Visual Cryptography". They extend their new scheme to privacy sharing problem. That paper is the seed of the visual cryptography and visual privacy distributing and every work was published in this area with the hint of this paper. In this paper abstract they said"We extend it into a visual difference of the k out of n privacy distributing Problem in which a dealer provides a clearness to each one of the n users any k of them can see the image by stacking their clarity, but any k-1 of them gain no information about it".

After this general concept many researchers find out different schemes for the visual cryptography [18]. This challenge goes to gray scale image to colour images and different ways and techniques were developed with incredible ideas. We will examine these all in our literature survey. However, this field is still growing in future based on the demand. The major demands are the security and low power computations at the time of decryption. Now days for the data security very famous and strong algorithm use. The main problem is the power usage at the time of decryption of these algorithms. We use many portable devices e.g. Laptop computer, mobile phone etc. these and many others are low battery power devices and need to use less there is battery power for increasing life time of the power usage. For this result the full fillment of this technology is rising. The locations of this field in the grouping of the Steganography are shown in the following figure1.

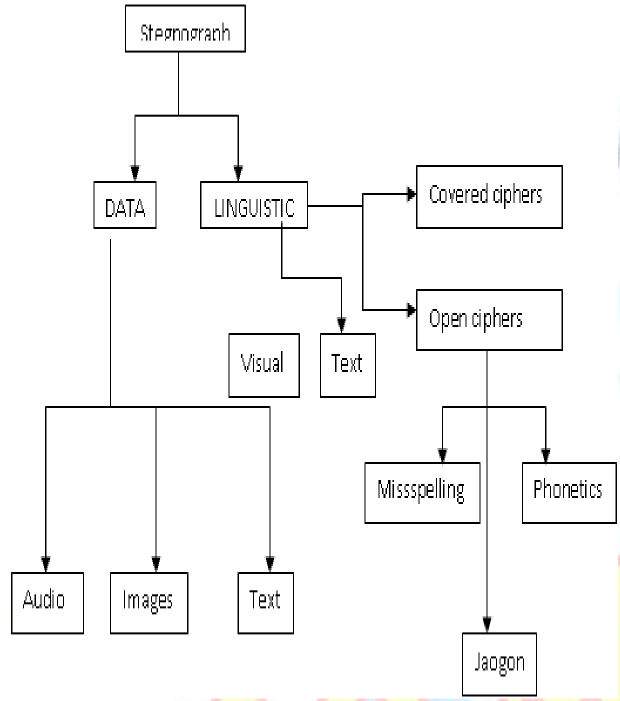


Figure: 1 Classification tree of Steganography

II. VC AND VSS MODEL

(Visual Cryptography and Visual Privacy Distributing Model)

The model for visual cryptography is mention by Naor& Shamir as follows:

1- A printed page of cipher-text and a printed transparency

2-The original cleartext is opened by placing the trans-patency with the key over the page with the cipher, allthough each one of them is identical from random noise.

The model for visual privacy distributing is as follows [3]:

1- There is a privacy picture to be shared among n participants.
2- The picture is divided into n clarities such that if any m clarities are placed together, the picture becomes visible.
3- If fewer than m clarities are placed together,

nothing can be seen.
4- Such a scheme is design by explore the privacy picture Most as a set of black and white pixels and handling each pixel separately.

A. Visual Cryptography scheme

Visual Privacy distributing scheme, there is a privacy picture to be shared among n participants. The picture is divided into n clarity such that if any m clarity placed together, the picture becomes visible. However, if fewer than m clarity placed together, or swapped by any other means; nothing can be seen [8]. Visual Privacy Distributing scheme uses mathematical privacy distributing but appliances in hardware, printed on clarity. It once created, it requires no technology, and however design and checking is lost [9].

B. Image halftoning

A halftone image is made up of a sequence of spots rather than a continual voice. These spots can be different magnitudes, different colours, and occasionally even different appearances. Larger spots are used to represent darker, denser areas of the image, while smaller spots are used for lighter areas. Colour half toning produces a halftone pattern for each of these inks. When these patterns are copied over each other, the human spectator will see a colour that cling on the aggregates of the colour inks. Visual cryptographic results run on binary or binaries inputs. Natural (continuous-tone) images must be first changed into halftone images by using the thickness of the net spots to replicate the original gray or colour levels in the target binary depiction. The halftone version of the input image is used instead of the original isolated image to produce the shares. The decrypted image is obtained by loading the shares together. Because binary data can be displayed either as frosted or crystalline when printed on clarities or viewed on the screen, overlapping shares that contain seemingly random information can reveal the privacy image without additional computations or any knowledge of cryptographic keys.

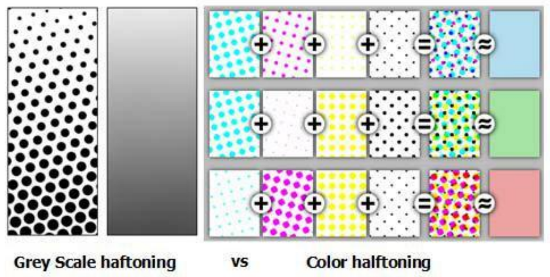


Figure 2. Image Halftoning.

C. Problems with algorithms

Because of the nature of the algorithm, the decrypted image is blacker, contains a number of visual impairments. of visual cryptography solutions expand the spatial aspiration of the privacy image. The necessity for inputs ofthe binary or hesitated nature only limits the applicability of visual cryptography. In above example, figure shows that the recover image has many impartments and relay as observable as the actual.

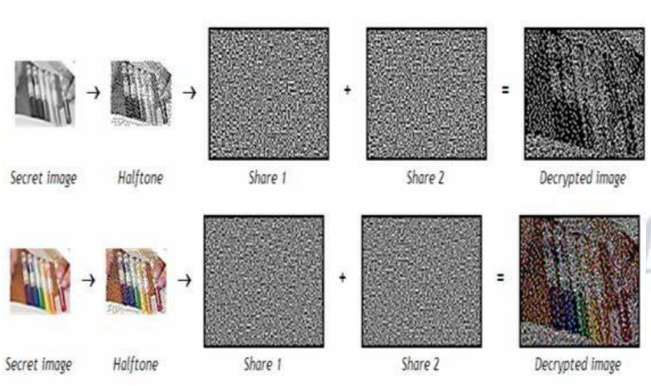


Figure 3. Example of Gray and color images.

III. Previous Work

In literature survey we studied the basic precisions and the start from those research papers that are the base of these technologies then review those papers that are presently available in this technology. Visual cryptography is a popular solution for image encryption. Using privacy issuing concepts, the encryption process encrypts a privacy image into the shares which are noise-like secure images which can be transferred or distributed over an untrusted communication channel. Using the properties of the HVS to force the identification of a privacy message from overlapping shares, the privacy image is decrypted without external computations and any knowledge of cryptography.

IV. Proposed Algorithm

We have design some schemes on visual cryptography and visual privacy distributing. Our approach for these schemes is randomization and pixel reversal. We have done several experiments and came up some new approaches of (2, 2) visual cryptography and (3, 3) visual privacy distributing schemes. First we explain the approach for the (2, 2) visual cryptography scheme. In (2, 2) visual cryptography scheme we have one privacy gray scale image (SI) as input to the algorithm. Where SI is considering as a matrix S_{ij} where i and j shows pixel positions and i, j= 1, 2, 3., n. All steps of algorithm in this scheme are shown below.

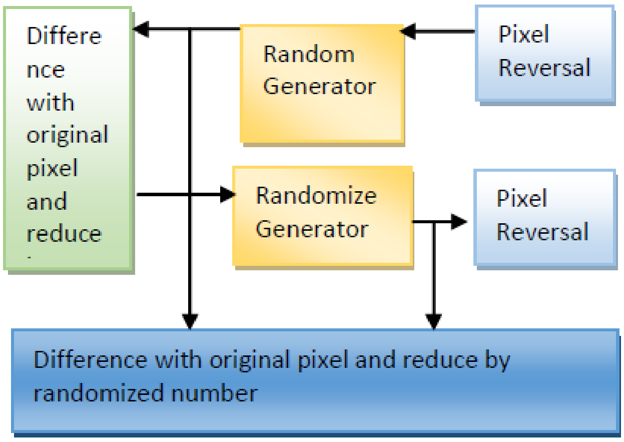
Step1- Pixel S_{ij} with position i and j is the input called original pixel.

Step2- Apply pixel reversal i.e.,S_{ij}' = 255 - S_{ij}.

Step3- Use random number generator (0.1 to 0.9) to decrease S_{ij}' randomly.

Step4- Take the difference of S_{ij}' with original pixel S_{ij}.

Step5- Use random number generator to reduce reversed value of S_{ij} ' randomly.


Difference with original pixel and reduce
Random Generator
Pixel Reversal
Randomize Generator
Pixel Reversal
Difference with original pixel and reduce by randomized number

V. Results

Results shows that the after giving the true gray scale picture as privacy image has better results in comparison of algorithm with outpreprocessing. Because for privacy image (true gray scale image) will reveal the privacy totally in shares in case of without preprocessing.

However, using pre-processing (half toning) the shares shows some information about the privacy. This can be improving to further by using extended preprocessing on the same processed image. The purpose of preprocessing is to preparing the image on a certain level that the algorithm must not reveal the privacy words from the image. The input is the

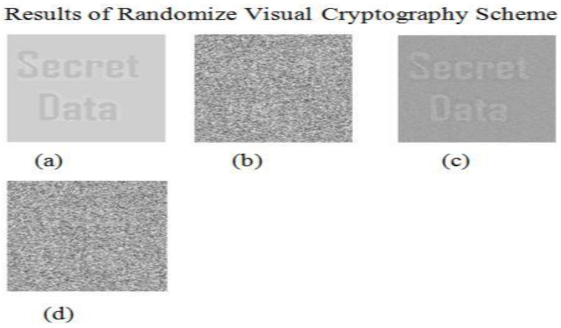


Figure 5. Randomize Visual Cryptography results: (a) secret image, (b) share 1, (c) share 2, (d) stacking of share 1 and share 2

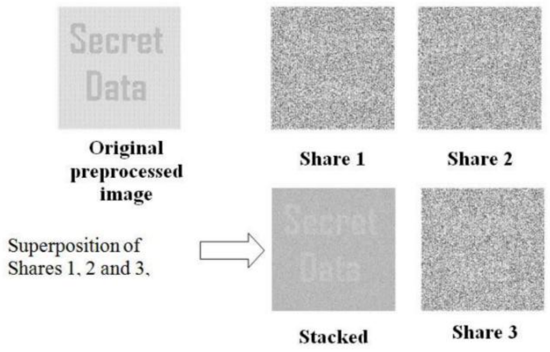

Secret Data
Original preprocessed image
Share 1
Share 2
Superposition of Shares 1, 2 and 3.
Stacked
Share 3

Figure 7 Randomize Visual Secret Sharing with preprocessing secret image

VI. Conclusion

We have shown that the (2, 2) randomize visual cryptography in practice where the shares are generated based on pixel reversal, random reduction in real pixel and subtractions of the original pixel with foregoing shares pixel. The original privacy image is separated in such a way that after OR operation of qualified shares we reveal the privacy image. In the (3, 3) visual privacy distributing scheme shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel and storing the final value of the share pixel after reversal into the shares in round robin fashion. The result of the three shares and after OR operation using stacking of all these qualified shares the original privacy reveal. We further mention the improvement of our algorithm regarding the acceptance of the true real gray scale image victoriously. Our schemes have shown less pixel expansion which is advisable and good for the final retrieval of the privacy image. Some contrast is change and impairments are still visible in the results of these schemes. Nevertheless by dividing the pixels into two or more sub pixel retrieve the privacy image with more impairments and bad resolutions. In our scheme the results are better then and the size of the retrieve image is the same as the original. Although size of pixel maximizes provides more easiness for alignment of the shares. This is the still researchable area to decrease this effect. Also our proposed schemes have shown high level of safety because of randomness.

VII. FUTURE WORK

The future work is to exceed the contrast and decrease the pixel expansion in the resultant privacy image. Later expands this work to use this technique with colour images. Also consider 3D images for making the shares who have partial privacy and divulge that privacy by stacking to every other.

REFERENCES

[1] Naor, M. and Shamir, A.,”Visual cryptography”, In Proc. Eurocrypt 94, Perugia, Italy, May 912, LNCS 950, pp. 112. Springer Verlag.,2010.

[2] Dmitri V.,”Digital Security and Privacy for Human Ruman Rights Defenders”, The International Foundation for Human Right Defenders, Manual, Feb. 2007

[3] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo ”Halftone Visual Cryptography via Direct Binary search” , Department of Electrical and Computer Engineering University of Delaware, Newark, DE, USA, 2010.

[4] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson, ”Visual Cryptography for general access structure”, ICALP’96, Italy, 1996

[5] Zhongmin Wang and Gonzalo R. Arce, ”Halftone Visual Cryptography Through Error Diffusion”, Department of Electrical and Computer Engi-neering, University of Delaware, Newark, IEEE, 2006.

[6] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, ”Half Visual Cryptography”, IEEE Transaction on image processing, vol. 15, no. 8, 2006.

[7] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, ”On the Contrast in Visual Cryptography Schemes”, Journal of Cryptology: the journal of the International Association for Cryptologic Research, 2009 .

[8] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptog-raphy to Financial Documents,technical report TR001001, Florida State University (2000).

[9] D Chaum, Privacy-ballot receipts: True voter-veriable elections, IEEE Security and Privacy, 2004,38-47.

[10] Nakajima, M. and Yamaguchi, Y., Extended Visual Cryptography for Natural Images, WSCG02,2002, 303