

Region Based Cryptography : A case of Segmentation Based Visual Cryptography

¹Yasir Choudhary, ² Amjed Khan Bhatti,

³ Sankait Gupta, ⁴ Irfan Jalal Bhat

¹Assistant Professor , Deptt. of Computer Application and IT ,Govt. P.G College Rajouri.

²Assistant Professor , Deptt. of Computer Application and IT ,Govt. P.G College Rajouri.

³Assistant Professor , Deptt. of Computer Application and IT ,Govt. P.G College Rajouri.

⁴Research. Scholar, Computer Application, Bhagwant Univeristy Ajmer (India)

ABSTRACT

Region growing is a simple region based image segmentation schemes. It also groups the pixels in whole image into sub regions (i.e. set to sub sets). This paper describes the various schemes of segmentation based visual cryptography and clear state that no proper method / schemes / techniques are used for proper type of images. In this paper, we have analyzed the region growing based image segmentation and the seeded growing area , but the quality of image is totally depend upon the way of selecting the seed i.e. automatically and manual way. As the seeded region growing techniques is gaining more popularity in practical day by day especially in medical images.

Keywords— *Image segmentation, region growing, security, seeded growing region, thresholding, fuzzy clustering.*

INTRODUCTION

Providing security to the digital information shared is an important issue in real life. Information gets more value when shared with others. Due to latest technologies related to networking and communication, it is possible to share the information like audio, video and image easily and hence the security of such information exchange is an important issues.

Unauthorised users or Attackers may try to access data or information and misuse it for different purposes. Various schemes for visual cryptography are proposed.

There are many techniques that are needed to prevent illicit usage of information. Such a techniques are known by secret sharing scheme. G.R Blakley and A. Shamir independently invented secret sharing schemes[1]. But in 1994 M. Naor and A. Shamir introduced the concept of visual cryptography[2]. The main concept of the original visual cryptography scheme is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k -out-of- n visual cryptography.

Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Visual cryptography (VC), proposed by Naor and Shamir [1], is a method for protecting image-based secrets that has a computation-free decryption process. In the $(2, 2)$ VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption process is performed by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations. In the above basic VC scheme each pixel 'p' of the secret image is encrypted into a pair of sub pixels in each of the two shares. If 'p' is white, one of the two columns under the white pixel in Fig. 1.1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image. By

stacking the two shares as shown in the last row of Fig. 1, if 'p' is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If 'p' is black, it outputs two black sub pixels.















Pixel	White 		Black 	
Prob.	50%	50%	50%	50%
Share 1				
Share 2				
Stack share 1 & 2				

Figure . 1.1- Construction of (2, 2) VC Scheme

Hence there is a contrast loss in the reconstructed image. However the decrypted image is visible to naked eye since human visual system averages their individual black–white combinations. The important parameters of this scheme are

- Pixel expansion 'm', which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.
- Contrast, which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image. Generally, smaller the value of m will reduce the loss in resolution and greater the value of 'm' will increase the quality of the reconstructed image.

As mentioned above if 'm' is decreased, the quality of the reconstructed image will be increased but security will be a problem. So research is focused on two paths

- To have good quality reconstructed image
- To increase security with minimum pixel expansion.

The following Types of visual cryptography and its extensions

- Visual cryptography for general access structures.
- Visual cryptography for gray level images.
- Recursive Threshold visual cryptography.
- Extended visual cryptography for natural images.
- Halftone visual cryptography.
- Visual cryptography for color images.

7. Progressive color visual cryptography.
8. Regional incrementing visual cryptography (RIVC).
9. Segment based visual cryptography.

LITERATURE SURVEY

Due to lost or steal of information is a big threat in present time. A lot of schemes are used to prevent the information from unauthorized access. In visual cryptography different techniques are used to avoid or illicit used of data (images). In some techniques pixels are used for encryption the images and also used of segment for encryption the images. In segment based visual cryptography segment are used to gives more security to images , as in segmentation uses the seven segment and sixteen display to gives the accurate result .Appropriate techniques are needed to prevent illicit usage of information. Such techniques are called as Secret Sharing Schemes.

G.R. Blakley and Adi Shamir independently invented secret sharing scheme in 1979[1]. When it comes to visual information like image, audio and video , then termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image based secrets. Moni Naor and Adi Shamir proposed the basic model of visual cryptography in 1994[2]. In which they stated/ express the idea how to send the image to other recipient without the any information lost/ steal. All shares are necessary to combine to reveal the secret image. There has been a steadily growing interest in visual cryptography. In 1997, a New Visual Cryptography Scheme for color images had been proposed by B.Sai Chandana, S.Anuradha[3] which can be used to hide the original image information from an intruder or an unwanted user. The images can be in any standard format. The encrypted image is sent to the destination through the network and then the image is decrypted. Symmetric key cryptography is used for this purpose. Experimental results indicate the proposed method is a simple, practical and effective cryptographic system. This method aims to build a cryptosystem that would be able to encrypt any image in any standard format, so that the encrypted image when perceived by the naked eye or intercepted by any person with malicious intentions during the time of transmission of the image is unable to decipher the image. The key used for this act is the symmetric key with minimum size of 47 bits. In 2006, D.Boen[4] proposed “Segmenting 2D ultrasound images using seeded region growing” in

which he express that an automatic way/ method of selecting seeds point is demonstrated and proof it effectively. he also eliminates the inherent order limitations bt processing pixels with same ∂ values in parallel. But the concept of the seven segment based display came into existence in 1908, but nobody paid attention towards its. In 2007, Bernd Borchert[6] brings the concept of segment based visual cryptography. He used the segments of image instead of pixels of images. He used to encrypt message that contains the symbol and shown by the segments bar i.e. consists of seven bar, in which three them horizontal and four of them vertical a as shown in figure 2. In 2011 I.S.Pallavi[19] proposed “Multiple Image Secret Sharing Scheme” in which she express the idea of how to handle multiple secret images in present time. she also handles encryption by intersecting / bisecting the secrets and managing the bisections using this concepts. In 2012, A.K. Mishra, A. Gupta and A. Kumar proposed “(n, n) Visual Cryptography based on Alignment of Shares” concludes that alignment is the best / important parameter in segmentation of visual cryptography. As in case if the required number of shares are not superimposed as per requirement alignment then the real image cannot be obtained still the real image inside the shares.

CONCLUSION

Segmentation Based Visual Cryptography is a dynamic approach for improving a security of transferring image data and it applies different segment display techniques like seven segment and sixteen displays and parallel seven and sixteen segment displays. If an attacker's try to recover the secret information in an unauthorized manner, these protocols are very effective for protecting the data. Because such attackers involves systematically checking all possible combinations until the correct key is found and every character in the share is generated using seven or a sixteen segment display and so it is very difficult to guess what character should be formed using these shares.

In another technique i.e. symmetric key cryptography both parties must have a secret key before the initial of encryption process. This improves the security of the exchange of information because nobody knows this secret key. It is only exchanged between the sender and receiver. So, symmetric key cryptography is another useful technique to improve the security of visual document exchanged.

References

1. Blakley, G. R., "Safeguarding cryptographic keys", Proceedings of the National Computer Conference, pp: 313–317, 1979.
 2. Naor M., and Shami, A. 1994, Visual cryptography, Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, pp. 1–12.
 3. B.Saichandra.et. al, A New visual cryptography scheme for color images international journal of engineering science and technology vol 2 (6), 2010, 1997-2000.
 4. David Boen, "Segmenting 2d ultrasound images using seeded region growing", 2006.
 5. T. Monoth and A. P. Babu, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion", In Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.
 6. Bernd Borchert, Klaus Reinhardt: Abh r- und manipulationssichere Verschl sselung f ur Online Accounts. Patent application DE-10-2007-018802.3, 2007 [Gr07]
 7. Geum-Dal Park, Eun-Jun Yoon , Kee-Young Yoo "A New Copyright Protection Scheme with Visual Cryptography", 2008 Second International Conference on Future Generation Communication and Networking Symposia, 2008.
 8. Debasish Jena, Sanjay Kumar Jena, "A Novel Visual Cryptography Scheme", International Conference on Advanced Computer Control, 2008.
 9. Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, , 2008 "Visual Secret Sharing For Multiple Secrets", Pattern Recognition 41 ,pp. 3572 – 3581.
 10. Daoshun Wang, Feng Yi, Xiaobo Li, 2009 "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42 (2009), pp 3071 – 3082,
 11. T. Monoth and B. Anto P. Tamperproof transmission of fingerprints using visual cryptography schemes. In Procedia Computer Science, volume 2, pages 143{148, 2010.
- J. Weir and W. Yan. Resolution variant visual cryptography for street view of google maps. In Proceedings of the ISCAS, pages 1695{1698, 2010