Analysis of Segmentation and Region Based Visual Cryptography

Dr. Amit Chaturvedi[*]   **Rashi Khanna**   **Vikas Choudhary**
Assistant Prof., MCA Deptt.,   M.Tech. Scholar   Assistant Prof., CSE Deptt.,
Govt. Engineering College, Ajmer,   Bhagwant University, Ajmer,   Bhagwant University, Ajmer,
Rajasthan, India   Rajasthan, India   Rajasthan, India

Abstract : Segmentation based visual cryptography is basically segment based cryptography technique rather than pixel based and it works on symbols that may be shown as segment display, the two major techniques proposed in this category are seven segment and sixteen segment display. The major benefit of using Segment Based encryption is that "It is easy to adjust the secret images and potentially easy to recognize for the human eye". We have summarized various schemes for segment based visual cryptography .We have analyzed majorly three techniques: 1) Secret sharing, 2) symmetric key distribution, 3) Seeded Region growing based segmentation. Future researchers may focus on automated seeded region algorithms. Region growing is a simple region based image segmentation scheme. It also groups the pixels of whole image into sub regions. This paper describes the various schemes of segmentation based visual cryptography and clearly state that there is no proper method / scheme that may be used for proper type of images. In this paper, we have investigate the region growing based image segmentation and the seeded growing area, but the quality of image is totally depend upon the away of selecting the seed i.e. automatically and manual way. As the seeded region growing techniques is increases day by day especially in medical images.

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

I. INTRODUCTION

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. Unauthorized users or Attackers may try to access data or information and misuse it for different purposes. 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 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.

Figure 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
   a) 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.
   b) 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.

Visual cryptography can provide feasible solutions with its ability to encrypt written materials such as printed text, handwritten notes and pictures perfectly in a secure way to decode the secret with the human visual system. The idea of visual cryptography is novel and unique in the area of computer science. The idea of visual cryptography involves the process of splitting the image into two separate images called shares and these shares are split in such a way that they do not give any clue about the original secret. The shares are stacked to recover the original secret back.
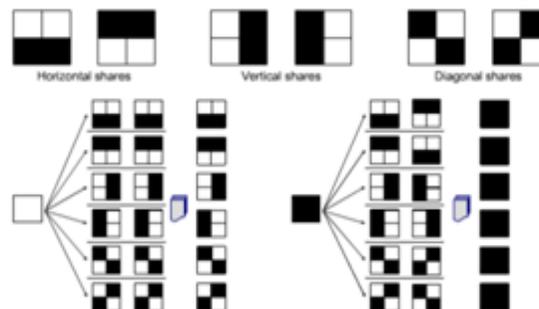

Figure 2 : Black and white pixel alignment in VC

On the other hand, a black pixel is also expanded to 4 sub-pixels with each share having two white and two black sub pixels. One of the two combinations of sub pixels will be randomly chosen to represent the pixel on each of the shares. However with the black pixels, the result of visually OR'ing the sub- pixels gives completely black pixels.share by itself does not disclose any information about the original secret as the sub pixels are evenly distributed on each share. When both the shares are stacked, the white areas of the original image appear grey and black areas remain black disclosing the original image. As each pixel is increased by 4 times the size of the originality the decrypted image is also increased by 4 times.

II. RELATED STUDY

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.

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.

S. Pallavi and Avandhani P S in 2012 proposed "A protocol for secret sharing using segment bases visual crypyography", They introduced the concept of the sixteen segment display in which the process for generating parallel segment depends on the type character or any character that is taken is convert into sixteen or seven segment display. As the proposed protocol is immune to brute or dangerous attack. Each character in the share that is converted looks like a sixteen segments display or seven segments display. The attackers cannot guess the character from the shares. S.Pallavi and P.S Avadhani in 2012[22] proposed the "Segment Based Visual Cryptography for Key Distribution" merges the positive aspects of segment display and visual cryptography for key distributions. Keys are very important for unauthorised access. They also express the paves a way for secure yet easy way of transferring secure with minimal human interference and accurate deliverance of data In 2013 S. Dhaliwal and A Jain proposed "A survey on Seeded Region Growing based Segmentation algorithms" that in which the survey the different seeded region growing based segmentations algorithms. They also shown the various algorithms which can be applied to segment a given image using region growing based algorithms as wrongly selected seed not give much accurate results.

In 2011, T. Zuva, Oludayo O. Olugbara, Sunday O. Ojo and Seleman M. Ngwira proposed "Image Segmentation, Available Techniques, Developments and Open Issues" in which they survey of, problems being encountered, achievements and the open issues in the research area of image segmentation and usage of the techniques / schemes in different areas/ ways. In this survey they also suggested what must be done in order for researchers to test their techniques '/ schemes performance and to compare them among other segmentation techniques / schemes. They considerd three main schemes / techniques Threshold-based, Edge-based and Region-based. Ans show the variations among them. In 2012 , R. Dass, Priyanka, S Devi "Image Segmentation Techniques" describes the different type of techniques of image segmentation as Gray Histogram Technique, Gradient Based Method, Thresholding Method etc. They also analyse the different algorithm for segmentation image. They also describes Recalculate position of Centroids in K clusters as $\mu i := 1\ (i)=j\ x(i)mi=1\ 1\ c(i)=j\ mi=1$ And gives a small process to follow.

In 2014, V.Vaithiyanathan and U. Rajappa proposed[25] "A Comparative Analysis among Basic Image Segmentation Methods" describes that segmentation has numerous methods that divide images which are widely apply to other applications i.e edge based, watershed segmentation ,threshold and clustering. They describes that the main purposes of segmentation is to less / reduce the image for esay analysis without the lost in original image. They also describes that every method or techniques of segmentation has its own importance and used depends upon requirement. In 2014, M. A. Hamdi Ecole " Modified Algorithm Marker-Controlled Watershed Transform for Image Segmentation Based on Curvelet Threshold" focus on the morphological operator called watershed segmentation.And later they used the low contrast image can be recovered by adaptive Threshold Curvelet.And this is beneficial for image segmentation. They said that segmentation is a process of divide the image into its characteristics e.g objects and color. In 2014, V.Vaithiyanathan and U. Rajappa proposed[25] "A Comparative Analysis among Basic Image Segmentation Methods" describes that segmentation has numerous methods that divide images which are widely apply to other applications i.e edge based, watershed segmentation ,threshold. and clustering. They describes that the main purposes of segmentation is to less / reduce the image for esay analysis without the lost in original image. They also describes that every method or techniques of segmentation has its own importance and used depends upon requirement.

III. PREPARE YOUR PAPER BEFORE STYLING

Segment display is a form of displaying decimal numerals. It is an alternative to the more complex dot-matrix displays. Segment displays are used more in electronic devices like digital clocks, electronic meters, and other electronic devices for displaying numerical information. There are different types of segment displays. viz,7-Segment Display, 9-Segment Display, 14- Segment Display, 16- Segment Display 7 Segment display[6] is the most famous and easy of all segment displays. 7 segment displays, as its name indicates, is a composed of seven elements. These seven elements are combined to produce representations of the Arabic numerals as shown in fig.3. The seven segments are arranged as a rectangle of two vertical segments on each side with one horizontal segment on the top, bottom, additionally, the seventh segment bisects the rectangle horizontally.
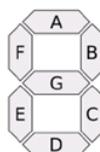

Fig. 3: Seven segment Display

The concept of Visual Cryptography has taken several forms in its transition. It started from a 2-out-of-2 secret sharing system and went to an m-out-of-n secret sharing system. Some tried to add steganography to Visual Cryptography, and some tried to move from black-and-white to color images[2][3][4][5]. There are lots of works which concentrated on pixel based images Visual cryptography is a budding topic. Visual cryptography is a simple and powerful method which can provide high security for confidential information. Recently, various studies about visual cryptography are proposed. Some has proposed a method for splitting the image into two different shares and some proposed on pixel quality enhancement [11][13], original image transmission or secret image transmission[12]. On the other hand, there have been also many reports for productions of meaningful binary halftone share images [14].Fu and Au have dealt with binary or ternary images like text images as secret image[8], while other many researchers have studied about natural gray-scale images like photographs as secret image and image as keys [9], [10]. A paper by Bernd Borchet [7] in 2007 has proposed a different variant of Visual Cryptography, i.e. instead of taking pixels as the smallest units to be encrypted, segments of a segment display are encrypted. The typical segment display is the seven-segment display, see fig.4, it is used to represent the digits 0; 1; 2; 3; 4; 5; 6; 7; 8; 9.

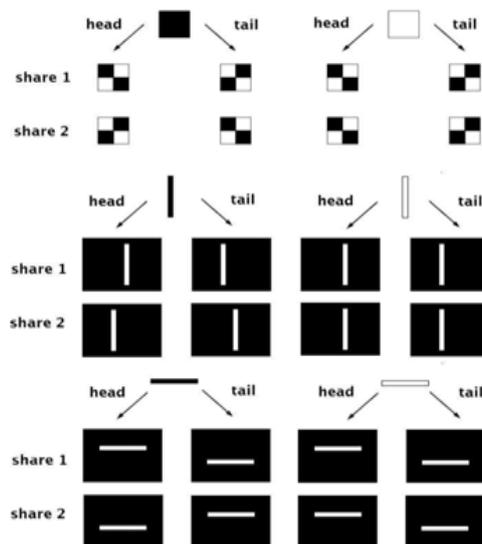Figure 4: Display of numbers using seven segments

Figure 5 : Pixel-based (above) vs. segment-based (center and below) Visual Cryptography

In present time, everybody wants that their information should be confidential from unauthorized accesses. whatsoever he / she send to others, other than the intended recipient can't see it and original quality should be obtained at receiver's end. Different techniques are used to improving the quality of original image to be obtained. As in segmentation based visual cryptography in which , a image is encrypted into segment and them send to recipient so that all (original image) may not lost and the original image are produced after decryption. In this techniques / schemes a different approaches are used in image to obtained the original image. The main concept of segmentation based visual cryptography was used 2007 by Borchert .This type of segment based cryptography is shown as figure 5.In this cryptography he takes the symbol 0 to 9 and all these symbol are made by digits 8, which consists as seven parallel bar and all the other digits are subset of the digits 8. A different types of approaches / schemes / techniques / methods are used in the segmentation based visual cryptography are as follow

- ➢ Segmentation Based on Edge Detection
- ➢ Gray Histogram Technique
- ➢ Gradient Based Method
- ➢ Region Splitting and Merging
- ➢ Thresholding Method
- ➢ Segmentation Methods Based on PDE (Partial
- ➢ Differential Equation)
- ➢ Region Based Segmentation Methods
- ➢ Mumford Shah Model
- ➢ Segmentation Based on Clustering
- ➢ C-V Model
- ➢ Segmentation Based on Artificial Neural Network
- ➢ Fuzzy Clustering
- ➢ Multi objective Image Segmentation
- ➢ Secret Sharing using Segment Based Visual Cryptography etc

IV. METHODOLGY

After analyzing the various schemes, the review is modeled and presented in the figure 6.   The different segments schemes are shown. Cryptography consists of video cryptography, audio cryptography and visual cryptography. Visual cryptography is further divide into different schemes which are all based on pixels based except the segmentation based visual cryptography and segmentation has some more techniques to improving the segmentation scheme .these schemes are Secret Sharing ,Symmetric Key Distribution ,Seeded Region growing based segmentation etc. The decryption process of Symmetric key Distribution is a very simple and easy for a nontechnical person to use. In this scheme, the shares are printed and stacked on each other to view the secret, the segments belongings to the first subset show transparent areas when the two shares are stacked. Therefore, after stacking, the number to be shown appears to the eye of the beholder. This scheme may be applied to print bank Personal identification number or other cryptographic key components that are necessary to keep the access of secret or confidential information of the individuals or organizations. Much research is required in the seeded region growing based segmentation that will automatically select the seed to segment the given image in an efficient manner. As the major issue in this scheme is the placing of a seed in seeded region growing segmentation. Multiple algorithms are proposed to segment a given image using region growing. In figure 7, which shows the various schemes of the image segmentation? Figure 7 also show that what happen with image when the seed is selected manual and automatically and if security is high or low.
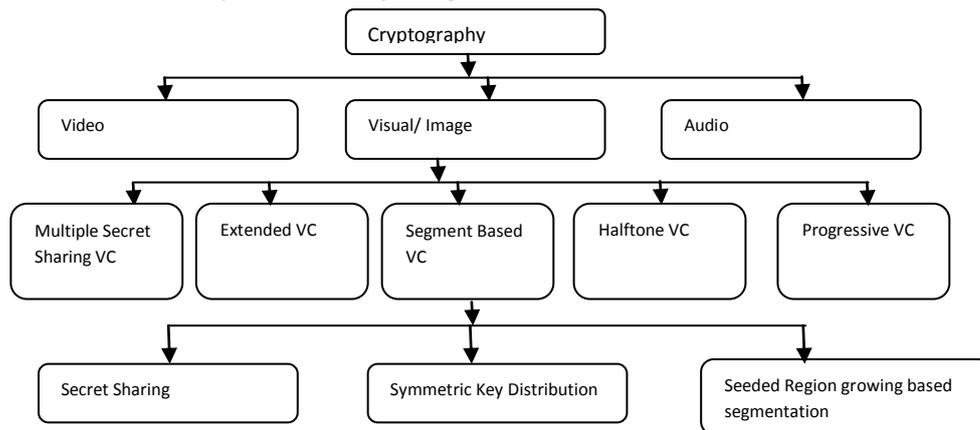

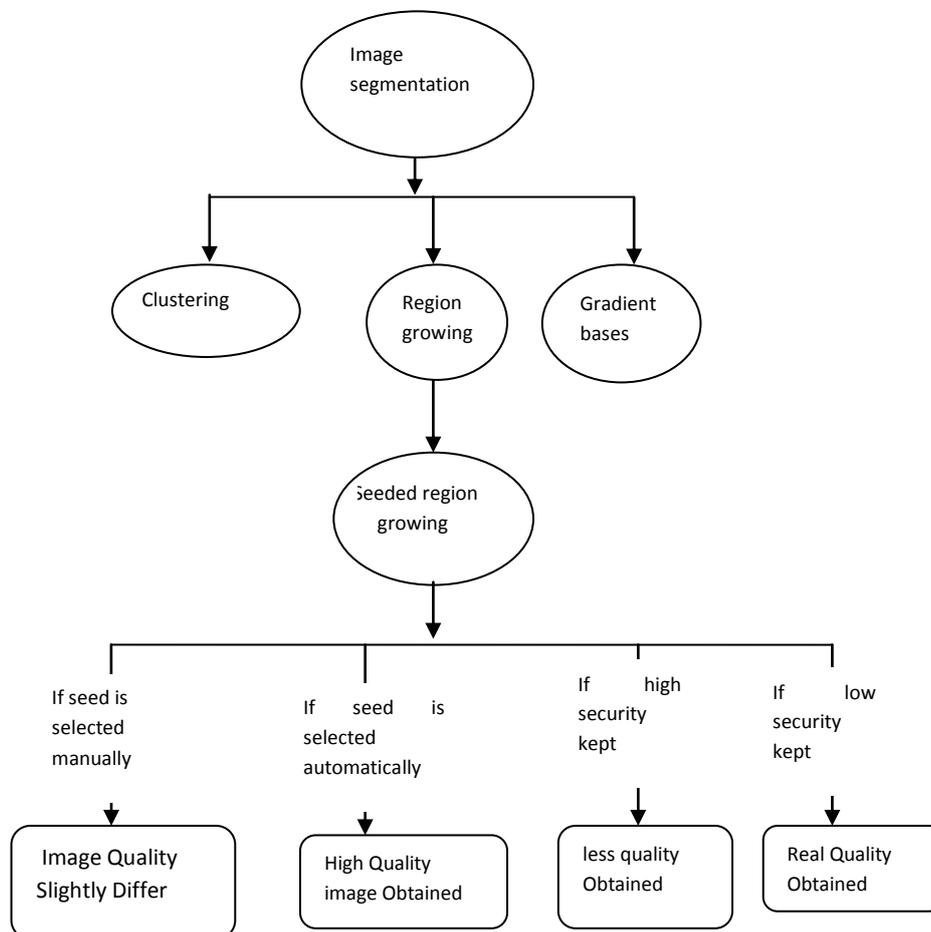Fig 6: Schemes for Segment Based VC

Figure 7: region growing schemes

V. 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.

The main goal of image segmentation is independent partitioning of an image into a set of disjoints regions that are visually different, homogeneous and meaningful with respect to some characteristics or computed property such as grey level, textual or colour to enable easy image analysis. The segmentation methods that are based on discontinuity properties of pixel are considered as boundary or edges based techniques that are based on similarity of homogeneity or region based techniques.

In future, a lot of work is still pending, regarding which schemes / method is used for which type of images. It is still a challenging issue. As in several decades researchers are known the factor affected the segmentation and still there is no universally accepted method for segment based visual cryptography. For us to find domain independent segmentation techniques is when we can evaluate the techniques by domain independent evaluation methods using a domain independent image database. In order for this to happen we need to create the universal image database such that researchers can use this database to evaluate their techniques. Whether a subjective or objective evaluation method is used the image database must be same and the images must be ranked to enable comparison of segmentation techniques. When researchers segment these images in the database they must indicate the value of parameters for each image segmented, the computational time and specification of the machine used. This will enable easy selection of segmentation technique for a particular area. Due to ad hoc form of research, this way of evaluating techniques will give some form of order in segmentation field. There is still room of improvement in each group of segmentation method.

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 IEEEInternational Conference on Information Technology, 2007, pp. 41-43.

[6]   Bernd Borchert, Klaus Reinhardt: Abh• or- und manipulationssichere Verschl• usselung 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 SharingFor Multiple Secrets", Pattern Recognition 41 ,pp. 3572 – 3581.

[10]   Daoshun Wang, FengYi, XiaoboLi, 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 fngerprints using visual cryptography schemes. In Procedia Computer Science, volume 2, pages 143{148, 2010.

[12]   J. Weir and W. Yan. Resolution variant visual cryptography for street view of google maps. In Proceedings of the ISCAS, pages 1695{1698, 2010.

[13]   T.R.Gopalakrishnan Nair Harikrishna Rai G.N. Gradient based seeded region grow method for ct angiographic image segmentation. 2011.

[14]   R.K.Krishna2 Shilpa Kamdi1. Image segmentation and region growing algorithm. pages 103-107.

[15]   Sunday O.Ojo Tranos Zuva, Oludayo O. Olugbara and Seleman M. Ngwira. Image segmentation, available techniques, developments and open issues. pages 20-29, 3, March 2011.

[16]   S. Cimato and C.N. Yang. Visual cryptography and secret image sharing. CRC Press,Taylor & Francis, 2011.

[17]   Vaibhav Choudhary, Kishore Kumar, Pravin Kumar, D.S. Singh " An Improved Pixel Sieve Method for Visual Cryptography", International Journal of Computer Applications Volume 12– No.9, January 2011

[18]   Masakazu Higuchi, Aya Emori, Shuji Kawasaki, Jonah Gamba, Atsushi Koike and Hitomi Murakami "Image Encryption Methods Using Intensity Transformations in Visual Cryptography", INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTERS IN SIMULATION Issue 1, Volume 5, 2011

[19]   Sesha Pallavi Indrakanti,Venkata Vinay Pragada, P.S.Avadhani,"Multiple Image Secret Sharing Scheme", 20th International Conference on Software Engineering and Data Engineering (SEDE-2011), Las Vegas, USA, on June 20-22. pp. 155-159, 2011,

[20]   Sesha Pallavi Indrakanti, Avadhani P.S.,"A Novel Multiple Visual Secret Data Hiding Scheme", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 2 (4) , july-August'2011, pp. 1423-1426.