Analysis of Schemes proposed for improving the Segment Based Visual Cryptography

Dr. Amit Chaturvedi[#1], Irfan Jalal Bhat[*2]

[#]*1Assistant Prof.MCA Deptt., Govt. Engineering College, Ajmer*

**2 M.Phil. Scholar, Bhagwant Univ., Ajmer*
Ajmer, India

Abstract
Segmentation based visual cryptography is segment based not pixel based and works on symbols that may be shown as segment display, the two major technique proposed in this category are seven segment and sixteen 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". In this paper we have summarised the various schemes for schemes for segment based visual cryptography given in figure 4 .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 seeding algorithms.

Keywords **:** Segmentation based Visual cryptography, pixel, cryptography, superimposed, security.

I. 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. Visual cryptography is the one of the simplest, secure and effective cryptographic scheme, which improves the users' trust on it.

These extensions to Basic visual cryptography model,

- Visual Cryptography Scheme, (k, n)
- Visual cryptography scheme for General Access Structure
- Visual Cryptography scheme for Grey images,
- Visual Cryptography scheme for color images,
- Multiple Secret Sharing Scheme,
- Extended Visual Cryptography scheme
- Recursive Threshold Visual cryptography scheme,
- Halftone visual cryptography scheme,
- Progressive Visual Cryptography scheme,
- Region Incrementing Visual Cryptography scheme
- Segment based Visual Cryptography Scheme.

This technique was latter expanded to a (m, n) scheme where someone who hold those n shares can see the secret, while *m* be the minimum set of shares that depend on *n*. To witness the secret clearly all the *n* should be present, combination of *m* shares also divulge the image but not with clarity. Each share is printed on a separate transparency, and decryption is performed by overlaying these disordered looking shares. When all *n* shares were superimposed, the original secret image would appear. If individual share is considered alone and the other share is unknown, it is a random collection of blocks. Given only one share, a second share cannot be crafted to reveal any possible image.

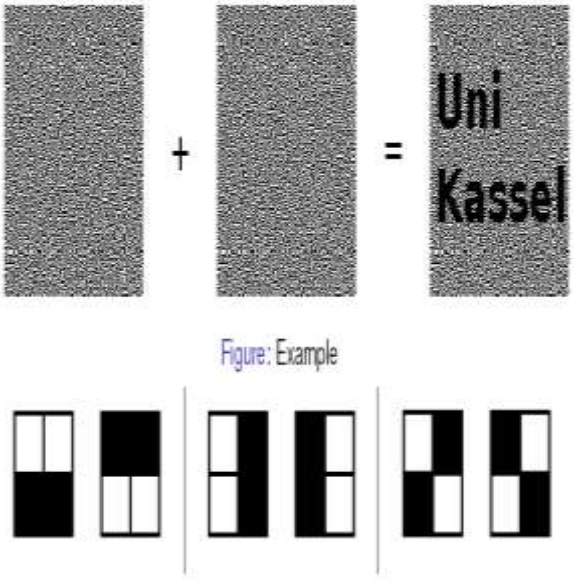

Fig 1: Pixel-based Visual Cryptography[2]

As shown in figure 1 the image is divided into shares so that the important information can't be revealed with only a few shares, all shares are to be combined necessarily. The shares consists pixels and these pixels are further divided into sub pixels which are either black or white. One image consists of the random pixels and the second image consists of the secret information. Separately these both are of no use but when superimposed or stacked together reveal the secret image back.

In this paper, we are presenting the analysis of the schemes and related issues of Segment Based Visual Cryptography.

II. Segment Based Visual Cryptography

A new version of Visual Cryptography is comes into existence, which is segment-based not pixel-based. It is used to encrypt messages (images) which are consisting of symbols that can be shown by a segment display. For example, the decimal digits 0 to 9 can be shown by the well-known seven-segment display. The benefits of the segment-based encryption are that it may be easy to adjust the secret images and that the symbols are potentially easy to recognize for the human eye, especially in a transparency-on-screen scenario. This approach proposed by Bernd Borchert[3], the messages consists of numbers that may be encoded by segment based visual cryptography using seven segment display. The seven-segment display was invented 1908. It uses seven bars, three of them horizontal and four vertical, arranged like an 8, see in Figure 2.

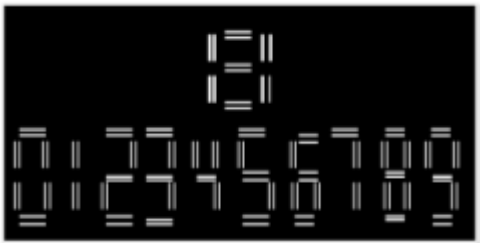

Figure 2: Seven Segment display

Some of the main benefits as compared with pixel-based Visual Cryptography are as follows:

- It is easy to adjust the two shares, especially in the case of a transparency-on-screen scenario,
- Very easy for the human eye to recognize the symbols, especially in the case of a transparency-on-screen scenario.
- A very low number of random bits are required, this may be a benefit, if real randomness (not pseudo randomness) is used in an encryption system.
- A layman (unknown person of the cryptography) can easily understand an encryption system and therefore trust segment-based Visual Cryptography than pixel-based Visual Cryptography.

Another example of pixels vs segment is shown as

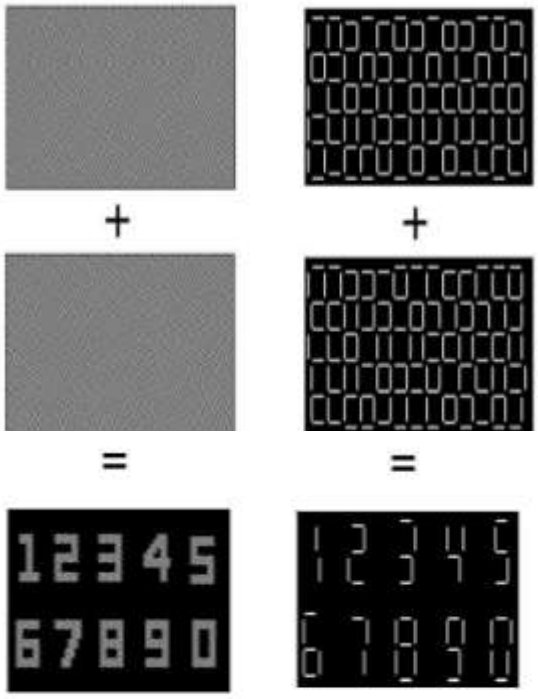

Figure 3: Pixel-based (left) versus segment-based (right) Visual Cryptography

In above figure 3, where the both techniques are used i.e pixel-based cryptography and segment

based cryptography in the image to show the different between the both techniques clearly.

III. REVIEW OF THE RELATED WORK

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.

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 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.

IV. MODEL AND METHODOLOGY

After analysing the various schemes, the review is modelled and presented in the figure 4.

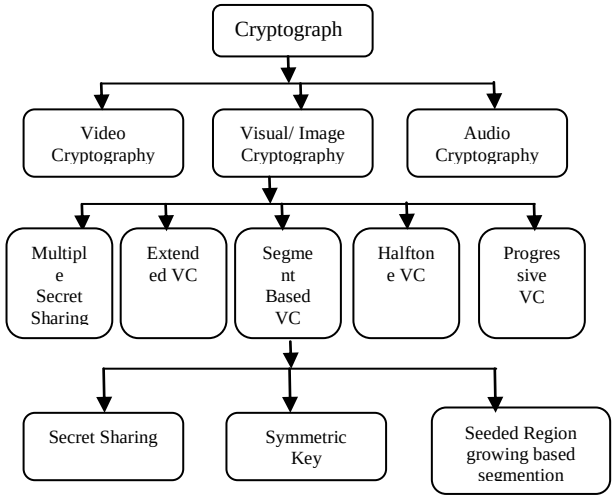

Fig 4 : Schemes for Segment Based VC

As in figure 4, 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 non-technical 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.

V. CONCLUSIONS

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 color 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.

The seeded region growing based segmentation algorithms is another approach for improving the results, placing seed in seeded region growing segmentation is a critical issue. So, future researchers may work on proposing such algorithms that will automatically select the seed and the seeded region in an efficient manner.

ACKNOWLEDGMENT

We feel grateful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript.

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.

[21] A. Ross and A. A. Othman, "Visual Cryptography for Biometric privacy", IEEE Transaction on Information Forensics and Security, vol. 6, no. 1, Mar.2011.

[22] Sesha Pallavi Indrakanti, P.S.Avadhani,"Segment Based Visual Cryptography For Key Distribution", International Journal of Computer Science and Engineering Survey (IJCSES), Vol. 3, No. 1, February 2012, pp.105-111.

[23] Sesha Pallavi Indrakanti, Avadhani P S.,"Privacy preserving through segment based visual cryptography", Advanced Computing: An International Journal (ACIJ), Vol. 3, No. 4, July 2012, pp. 95-103.

[24] M.Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012 218.

[25] V. Vaithiyanathan a 1 nd 2U. Rajappa "A Comparitive Analysis among Basic Image Segmentation Methods" World Applied Sciences Journal 29 (Data Mining and Soft Computing Techniques): 155-158, 2014 ISSN 1818-4952

[26] Prasad D. Baitule and Swapnil P. Deshpande " A Survey On Efficient Anti Phishing Method Based on Visual Cryptography Using Cloud Technique By Smart Phones" International Conference on Advances in Engineering &Technology – 2014 , pp .11-15

[27] I.D JUDITH Dr.G. J. Joyce Mary "ANTI PHISHING METHOD USING VISUAL SECRET IMAGES" International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163Issue 1, Volume 2 (January 2015).

[28] R.V.Prasad CH1, S.Suresh Nimra Nagar,Ibrahimpatnam,Vijayawad A COMPREHENSIVE IMAGE SEGMENTATION APPROACH FOR IMAGE REGISTRATION, *International Journal of Computer Trends and Technology- volume3Issue4- 2012*