PRIVACY PRESERVING THROUGH SEGMENT-BASED VISUAL CRYPTOGRAPHY

Sesha Pallavi Indrakanti[1] and Avadhani P S[2]

[1]Department of Computer Applications, GVP Degree College (Autonomous), Visakhapatnam.
ipallavi@yahoo.com

[2]Department of Computer Science and Systems Engineering, Andhra University College of Engineering (Autonomous), Andhra University, Visakhapatnam.
psavadhani@gmail.com

ABSTRACT

The role of privacy in the digital world is an essential criterion and confidentiality of pictographic data has added significance to the study of security. A version of visual cryptography for hiding textual data which is based on sixteen segment display is presented. The secret that is in the form of alpha numeric and special characters is converted into segment display and is then encrypted into two random shares. The decryption process involves the stacking of these two shares. The process of key distribution becomes much easy and secure with this concept.

KEYWORDS

Visual cryptography, Sixteen-segment display, Segment, Key distribution, password, Encryption, Decryption.

1. INTRODUCTION

The world of security presents an ocean of challenges which insist on constantly new and outstanding encryption techniques. This has a top priority in applications which require transferring of sensitive data. 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.

Various visual cryptography threshold schemes have been proposed since it was first introduced by the scientific community of Naor and Shamir during May 1994 at Eurocrypt'94[1]. Their proposed scheme described a new type of cryptographic scheme which encodes a black and white image into shares and the decoding process involves the of stacking of the transparencies on the top of each other .Of the different schemes proposed 2 out of 2 scheme is the basic scheme and others are 3 out of 3 scheme, a 'k' out of 'k' scheme and a general 'k 'out of 'n' scheme.

DOI : 10.5121/acij.2012.3412

To witness the secret clearly all the n shares are required, a combination of k shares also divulge the image but not with clarity. Each share is printed on a separate transparency, and decryption involves the superimposing of the n shares to see the original secret.

If individual share is considered alone and the other share is unknown, it looks like a random collection of blocks. Knowledge of one share cannot help in the crafting of the second share to reveal the secret image. Therefore, individual shares reveal no information about the original image. Each pixel is replaced with four pixels, so the image gets blown up to four times the original size. Then the image is encoded into shares.

On the proper stacking of shares, the sub pixels for the white pixel are visually OR'd to produce the result as shown in figure 1.It is clear that the resultant expanded white sub pixel is a combination of two black and two white sub pixels. The white pixel in the shares generated also have two black and two white pixels in them. This white pixel results in the appearance of a grey with noise in it.

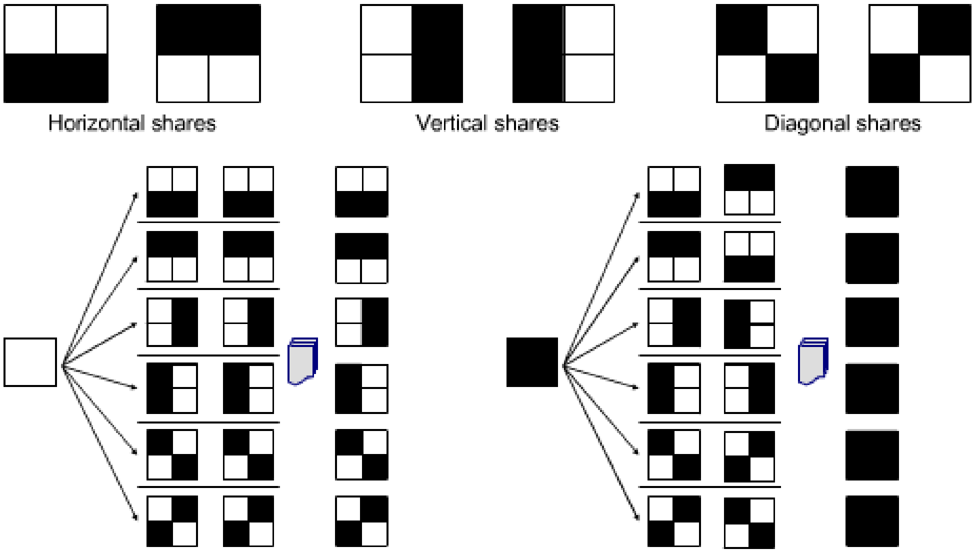

Figure.1 Black and white pixel alignment in visual cryptography

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.

A 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.

The standard visual cryptography scheme is limited to black and white images. Naor and Shamir[1] have applied this idea on black and white images only. The present day wants have out grown black and white images. The change in the technology insists on color image encoding schemes. There are many challenges that have been taken to encrypt color images.

In 1997 Verheul and Tilborg [2] proposed an algorithm for encrypting color images taking color palette that contains c different colors. A pixel in the image will take on one of the c colors. Encoding process involves c sub-pixels to be randomly placed in share one; another c sub-pixels are placed in share two. The disadvantage with this scheme is that when the shares are stacked, 1 out of the 16 color regions will let the true color and the remaining 15 regions will be black. This results to a decrypted image that is mostly black with pin points of red, yellow, green and blue. Thus the quality of the recovered image is considerably bad. Yang &Liah in 2000[3] improved the pixel expansion to c*2 where it was c * 3 in Verheul and Tilborg [2] scheme. But the shares generated still carried noise. Chen Chang [4] in 2005 developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more efficient way to hide a gray image in different shares. In this scheme, size of the shares is fixed and it does not vary even when the number of colors appearing in the secret image differs. Scheme does not require any predefined Color Index Table. Though pixel expansion is fixed on this scheme it is not suitable for true color secret image. To hide a color secret image in multiple colored images it is desired that the generated camouflage images contain less noise. For this purpose R.Youmaran et al[5] in 2006 invented an improved visual cryptography scheme for hiding a colored image in multiple colored cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with the similar quality of the originals. I.S.Pallavi et al [6] in 2007 proposed Secure Visual secret sharing scheme, this approach uses meaningful shares (cover images) to hide the colored secret image that is split in to two parts thereby also reducing the threat of vulnerability.

The techniques discussed till now are all about sharing a single color secret. Chang et al in 2000[7] suggested that visual cryptography scheme should support wide image format like color and gray scale. They also proposed that random looking shares appear suspicious and thus are vulnerable to attacks by attackers. Pei-Fang Tsai and Ming-Shi Wang on 2006[8] proposed a technique for “Hiding Three Secret Data.” Jen-Bang Feng et al [9]in 2008 suggested that VCS should support multiple secrets to work efficiently. Daoshun Wang et al [10] provided general construction for extended visual cryptography schemes using matrix extension algorithm. A general construction method for single or multiple and binary, grayscale, color secret images using matrix extension utilizing meaningful shares was suggested. If one schemes support only one secret to share at a time to share multiple secret images numerous shares has to be generated, transmitted and maintained. I.S.Pallavi et al[11] in 2011 proposed “Multiple Image Secret Sharing Scheme”, which handles the present trend of encrypting multiple secret images. This scheme handles encryption by bisecting the secrets and managing the bisections. I.S.Pallavi et al[12] in 2011 proposed “Permutation based Image Encryption Technique” in which a secret is encrypted into meaningful shares and a key is constructed based on the encryption.

2. SEGMENT DISPLAY

Segment display is a form of displaying decimal numerals; it is an alternative to the more complex dot-matrix display. 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 displaysviz.,7-Segment Display, 9-Segment Display, 14-Segment Display and 16- Segment Display.

Sixteen segment is an extension of the seven segment. It adds four diagonal and two vertical segments and splitting the three horizontal segments in half. A fourteen-segment display splits only the middle horizontal segment where as the sixteen segments display splits the three horizontal segments into half. This splitting adds flexibility to display in representing a variety of alphabets and characters. As seven segments cannot represent all the characters of English and fourteen segment displays cannot represent all the character of English in lower case. Sixteen segment display over comes the problems faced with seven and fourteen segments. Figure 2, shows the typical representation of sixteen segments display. Sixteen segments are also called as “Union jack display”.

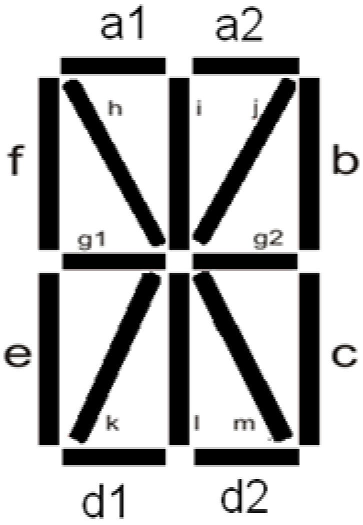

Figure 2

3. PRIVACY PRESERVING THROUGH SEGMENT-BASED VISUAL CRYPTOGRAPHY

The word password has become synonymous security. These words or phrases are our keys to the digital world. These secret codes help us in identifying friend to a foe, and are vital for modern living, as these are used in all walks of our life viz., checking, sending or receiving emails, withdrawing money from an ATM or to connect to our online mobile banking accounts.

The usage of the secret code is preempted by two stages, one being the building of an efficient password and the latter its distribution. In the building of the secret code, character diversity is a key component of strong passwords as it reduces the predictability and weakness of the passwords. Usage of alpha numeric and special symbols in passwords can enhance the uniqueness of a password. These passwords or PINs are usually transmitted to the third party through a courier or personally. Over time the need for cryptographic speed has increased and with this came a requirement that ensured the need to frequently change keys to prevent discovery and compromise in security. Physical delivery of keys is an out of bounds issue with the increase in the number of users and machines.

The first proposed solution for this problem was by Diffie and Hellman [13] in 1976.This protocol uses two sets of mathematically related keys and a complex mathematical equation that takes advantage of this relationship. This secret key can be used independently to generate a number of asymmetric keys that the two computers can use to encrypt data travelling from one to the other. An alternative technique suggested for the trusted transfer of this password or key is with the help of a technique called “Privacy Preserving through Segment Based Visual Cryptography.”

A paper by Bernd Borchet[14] 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. A paper on "Segment based visual cryptography for Key Distribution" proposed on Sesha Pallavi Indrakanti and Avadhani P S [15] in 2012 has taken a seven segment display and applied it key distribution which has numericals. This technique is appropriate for maintaining secrecy of the initial exchange of key. The restriction being the non usage of alphabets as they cannot be properly represented using seven segments.

In the process of visual cryptography every picture is viewed as one or more shares, the idea is to send or communicate the shares separately so that the image can be reconstructed from the shares at the other end. A methodology to divide any symbol represented by sixteen segment display as shares so that the same idea of visual cryptography can be used for secured transmission and authentication. Parallel segments are generated by drawing two single segments S1 and S2, drawn in white on a black background, close and parallel. Figure.3. shows the parallel segment display of a sixteen segment display.

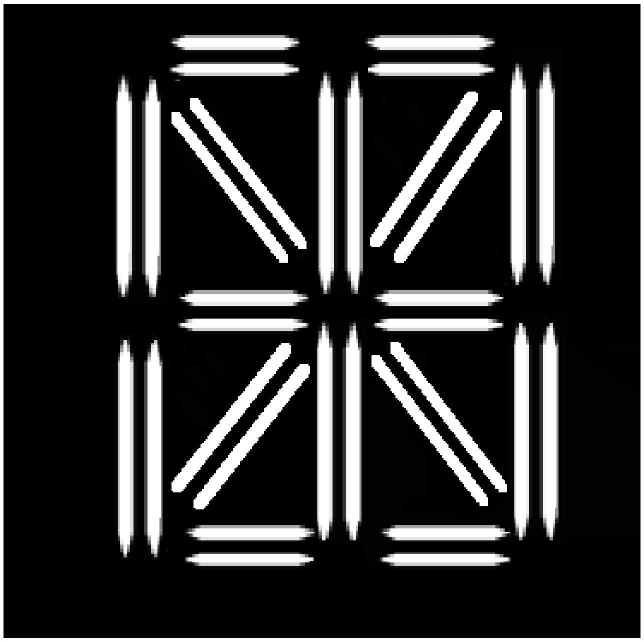

Figure.3: Parallel Sixteen Segment Display

The first share is randomly generated like that of pixel-based visual cryptography, this means from every pair of parallel segments either S1 or S2 are selected randomly depending on the symbol to generate the share. Sixteen segment display has diagonal segments, that give the flexibility to symbolize the alphabets more appropriately.

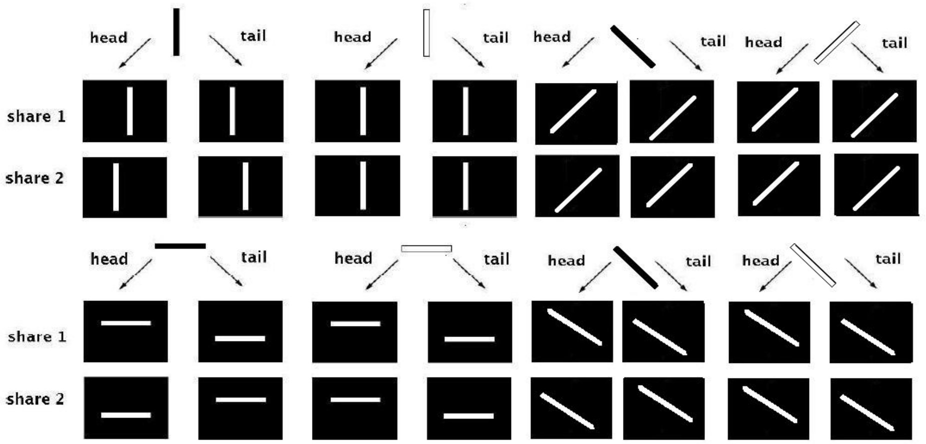

Figure.4. Combinations of horizontal, vertical and diagonal shares.

The association of shares in segment display for a sixteen segment display is shown in figure 4. There are eight different combinations of shares in which two represent vertical, two represent horizontal two represent right diagonal and two represent left diagonal shares each. Each type of segment has a black and a white combination. A black vertical or horizontal or diagonal line can be produced by placing the segments parallel to each other, where in two segments have to be superimposed to get a white vertical, horizontal or diagonal line. The parallel segments with two grey lines reflect a black segment. The two intersecting lines represent a white single line and this reflects a white segment.

As the advantages of segment based visual cryptography to that of pixel-based visual cryptography are prominent, the positive aspects of visual cryptography and sixteen segments display for preserving the privacy of passwords will be discussed here. Distribution of passwords securely is a challenging job and they are more vulnerable in insecure networks. A process of secure key distribution is discussed here. The password can be of any size composed of alpha numeric and special characters.The process of segment based visual cryptography is applied to visual cryptography and used in secure distribution of passwords. For a secure communication to be established between two parties, the initial phase requires the secret key to be distributed between both the parties. In case of symmetric key there is one single key. The same key has to be distributed to the sender and receiver. Usually a trusted third party is employed in the generation and distribution process. This technique concentrates on the secure distribution of the secret key.

According to this technique the secret which is composed of alpha numeric and special characters is made into two shares and one share is distributed to the customer and the other is kept with the trusted third party. The process of key learning will involve both the customer and the trusted third party. The customer authenticates himself and learns the secret from the share with him and the one with the trusted third party. Once the key is learnt the customer will proceed forward with the process of secure communication.

The key is generated using parallel segments of the sixteen segment display and the shares are generated by parallel segments, at most one of the parallel segments is chosen randomly depending on the symbol to generate the share. The chance of guessing the characters is almost nil as each character in the share looks like a sixteen segment display. Generation of share 2 is based on share 1.

The following are the steps of the algorithm for generating a segment based password using sixteen segment display.

Step 1: Type or browse a unique secret code which is made up of English alphabets of both cases,
numbers and special characters.

Step 2: Every S segment of the character in the text is split into two segments S1, S2 that are parallel. The two parallel lines should be white in color on a black surface.

Step 3: Following step 2 Generate the segment display of the text in step1.

Step 4: Share 1 is generated randomly i.e., either of the parallel segments is generated randomly. The randomly generated segment is kept white and the parallel segment is made black.

Step 5: Share 2 is generated based on share 1.

Step 5.1: If segment S belongs to this subset then the selection is the same as that in the random share and alternative segment is turned black.

Step 5.2: If the segment S does not belong to the subset then the alternative segment of the one in the random share is selected and random shares segment is made black.

4. RESULTS

If the text to be submitted for segment display is "Turnleft$Turnright%5" the parallel segment representation of this phrase is shown in figure 5. This parallel segment display is subjected to the encoding process and results in two shares, share 1 is shown in figure 6 and share 2 is shown in figure 7. The secret cannot be recovered from one single share as each character in the share each look like a sixteen segment display. The chances of applying brute force and identifying are nil. Figure 8 shows the result of stacking the share 1 and share 2.

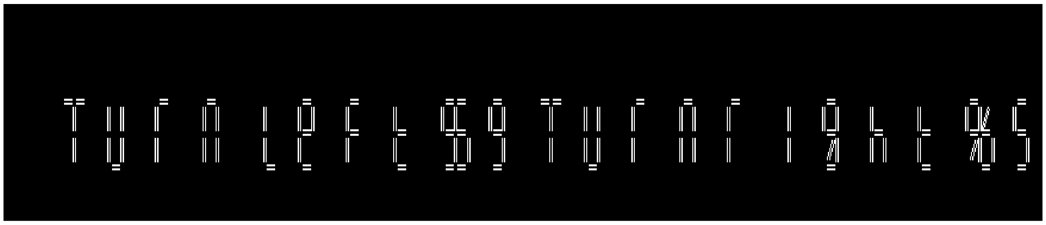

Figure 5. Parallel segment Display of the secret

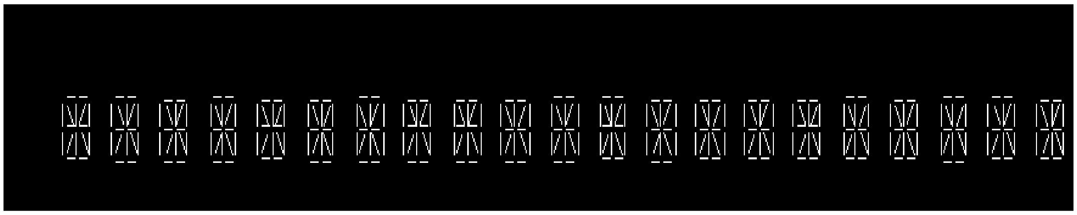

Figure 6.Share1

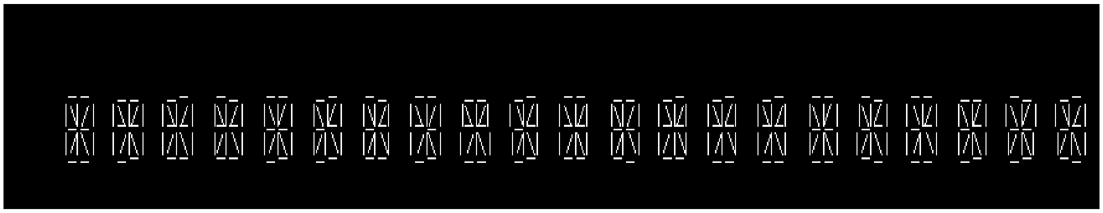

Figure 7.Share2

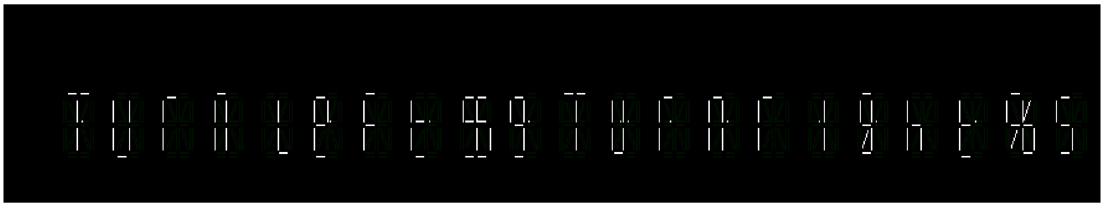

Figure 8.Result of stacking share1& share 2

5. CONCLUSIONS

Segment-based visual cryptography addresses some of the pitfalls of pixel based visual cryptography with reduction in decryption process time being one and the secret being much more clearly visible to normal human eye being the other. This concept proposes a secure yet easy way of transferring data with nil chances of guessing attacks.

REFERENCES

[1] Naor, M. and Shamir, A. 1994, Visual cryptography, Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, pp. 1–12.

[2] E. Verheul and H. V. Tilborg,1997 "Constructions And Properties Of K Out Of N Visual Secret SharingSchemes." Designs, Codes and Cryptography, 11(2) , pp.179–196,.

[3] C. Yang and C. Laih,2000 "New Colored Visual Secret Sharing Schemes". Designs, Codes and cryptography, 20,pp. 325–335.

[4] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin ,2005"Sharing A Secret Two-Tone Image In Two Gray-LevelImages", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05).

[5] R.Youmaran, A. Adler, A. Miri ,2006"An Improved Visual Cryptography Scheme For Secret Hiding", 23rdBiennial Symposium on Communications, pp. 340-343,.

[6] I.S.Pallavi, P.S.Avadhani,2007 “Secure Visual Secret Sharing Scheme”, in proceedings of 10th world conference on Integrated Design and Process Technology held at Antalya, Turkey during 3rd –8th June, pg,no323-325.

[7] C. Chang, C. Tsai, and T. Chen.2000 “A New Scheme For Sharing Secret Colour Images In Computer Network”,Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July.

[8] Pei-Fang Tsai, Ming-Shi Wang, 2006“An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data,” in Proceedings of JCIS'

[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]Sesha Pallavi Indrakanti, Venkata Vinay Pragada, Avadhani P.S,2011 “Multiple Image Secret Sharing Scheme”, in 20th International Conference on Software Engineering and Data Engineering (SEDE-2011), Las Vegas, Nevada, USA during june 20th –22nd , Published in proceedings pg no 155-159.

[12]Sesha Pallavi Indrakanti, Avadhani P.S,August 2011,”Permutation based Image Encryption Technique” International Journal of Computer Applications (0975 – 8887)Volume 28– No.8, pg no45-47.

[13] W. Diffie and M. E. Hellman,Nov. 1976, ‘New Directions in Cryptography’ IEEE Transactions on Information Theory, vol. IT-22, ,pp: 644–654

[14] Bernd Borchert,WSI-2007-04“Segment-based Visual Cryptography” WSI-2007-04.

[15]SeshaPallaviIndrakantiAvadhani P.S,, February 2012,” Segment Based Visual Cryptography for Key Distribution” International Journal of Computer Science & Engineering Survey (IJCSES) 2012 Vol. 3 No. 1, February ’2012, pg.no105-111

Authors

Sesha Pallavi Indrakanti received her M.Sc. degree from Andhra University 2002. She received her M.Tech. degree in Information technology in 2007 from Andhra University. She has an experience of 10 years in teaching and is presently working as Associate professor and Head of the Department of Computer Applications in G.V.P.Degree College (Autonomous),Visakhapatnam, India.She is pursuing her Ph.D. from Andhra University, Visakhapatnam, India.Her areas of interest are Network Security, Data communications & Networks and Operating Systems.

Prof. P.S.Avadhani did his Masters Degree and Ph.D. from IIT Kanpur. He is presently working as a Professor in the Department of Computer Science and Systems Engineering, Andhra University college of Engineering (Autonomous),Visakhapatnam. He has more than 75 papers published in various national/ international journals and conferences. His research areas include Cryptography, Data Security, Algorithms, and Computer Graphics.