ISSN:0975-9646

Secure Color Visual Secret Sharing Scheme Using Shifting Coefficient with No Pixel Expansion

John Justin M, Manimurugan S, Alagendran B

Department of Computer Science and Engineering,
Karunya University,
Coimbatore,India

Abstract-The focus is to design a framework for a color visual secret sharing scheme highlighting towards its security and pixel expansion problems. A Secret image has been diffused in between two meaningful cover images called share images. The participant who stacks both the share images can only obtain the secret image. In addition to that an extra confidential image has been embedded in share images to provide additional security in promoting the authentication to the participant and it carries the lifetime of the secret image. To reveal the extra confidential image, place the first share constantly and shift the second share to some unit. In this Paper a shifting coefficient value has been introduced to shift the second share image to certain unit, here the shifting coefficient acts as a key in-between the participant without which the Extra confidential image will not be revealed, which promotes good level of security also no pixel value has been expanded throughout the process.

Keywords-Visual Cryptography, Visual Secret Sharing Scheme, No Pixel expansion, Shifting Coefficient.

I. INTRODUCTION

Internet is important but insecure platform for communication. Many digital images that carry secret information are transmitted via internet. Hence it becomes common, sending secret information through internet in our day to day life. Once if the Secret information is leaked to unauthorized users then it leads to unpredictable loss to the owner or participant. For example, if the bank accounts detail or credit card information were leaked then it leads to financial risk. Therefore it is necessary to secure the secret information while transmitting it through internet. For securing the information many encryption algorithm has been proposed earlier like conventional cryptosystem such as AES(Advanced Encryption Standard),DES(Data Encryption Standard),ECC (Elliptic Curve Cryptography),RSA (RSA) they are vulnerable to the attacks perform by the attackers one or in the other way. In order to meet this vulnerability data hiding scheme like visual secret sharing scheme has been proposed. Visual Secret Sharing actually hides a secret image in two cover images called share images and sends it via internet; the participant at the receiver end stacks both the image to reveal the secret image. Mainly it does not need any computation work rather the secret image can be viewed by the human vision. The extra confidential image is revealed by placing the first share image constantly and shifting the second share image to certain units by using the shifting coefficient value introduced in this paper. The shifting coefficient is a key like structure added during the embedding of the extra confidential image into the cover images and the key value is needed while extracting of the share images to reveal the extra confidential image.

II. LITERATURE SURVEY

Der Chyuan Lou et al proposed a visual secret sharing scheme with authentic ability using the non expanded meaningful shares. Along with the hiding of secret image in two cover images which are called share images, this method embeds an additional confidential image in share images. the secret image by placing it one on another. Then first share image is kept constant and another share image is shifted for certain unit to obtain the extra confidential image which holds the validity and the data about the data of the revealed secret image. The main advantage is using the color images with no pixel expansion.[1] Y. F. Chang et al has jointly proposed a data hiding scheme using the pixel swapping method for Halftone images. In this paper, promotes the halftone share image with high clarity and the secret image can be viewed directly by the human eyes by attacking each shares. This paper proves the

good level of increase in terms of quality of the obtained secret image when compared with the other existing techniques.[2]

Hsien Chu Wu et al has put forth a visual cryptographic method for color images using the meaningful shares. In this paper, the halftone technique is used along with the (CCT) cover coding table and (SCT) secret coding table for generating the meaningful shares to avoid the attention of the hackers or attackers. Here the secret image is obtained by superimposing the two share images one on another. Results shows good achievement in attaining good range of security.[3]

Shyong Jian Shyu has designed a framework for Image encryption by using random grids. When compared to the existing visual cryptography schemes, this algorithm does not need any basis matrices for encoding the shares. Hence the pixel expansion problem has been fixed.[4]

A novel secret image sharing scheme for the true color images with size constraint was proposed by Du-Shiau Tsai. In this paper, the combination of neural networks with the variant visual image secret sharing scheme, the quality of the revealed secret images and camouflage images were observed to be the same to its appropriate original images. Experimental results proves the feasibility of the method.[5]

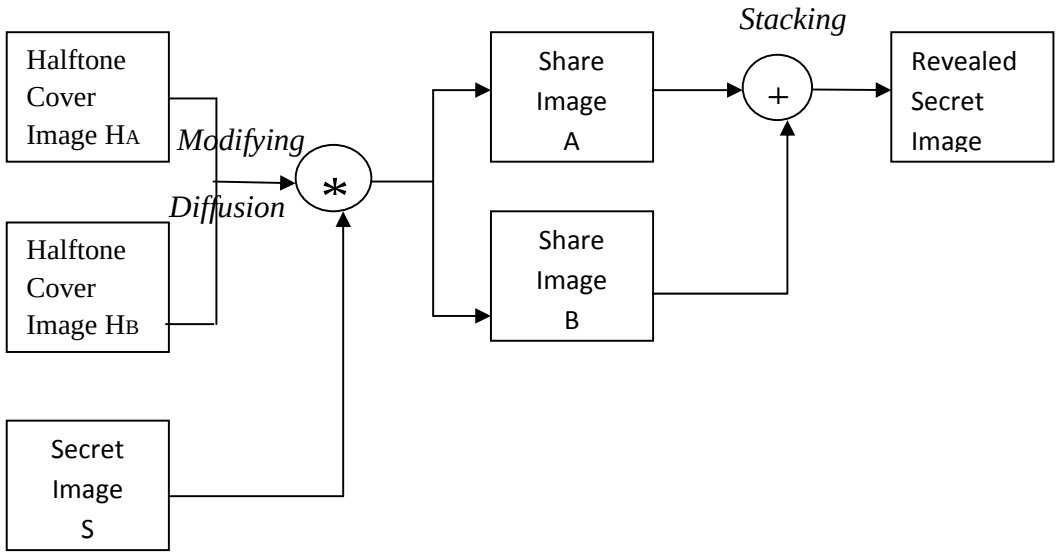


Fig 1. Block diagram of Der-Chyuan Lou et al's model [1]

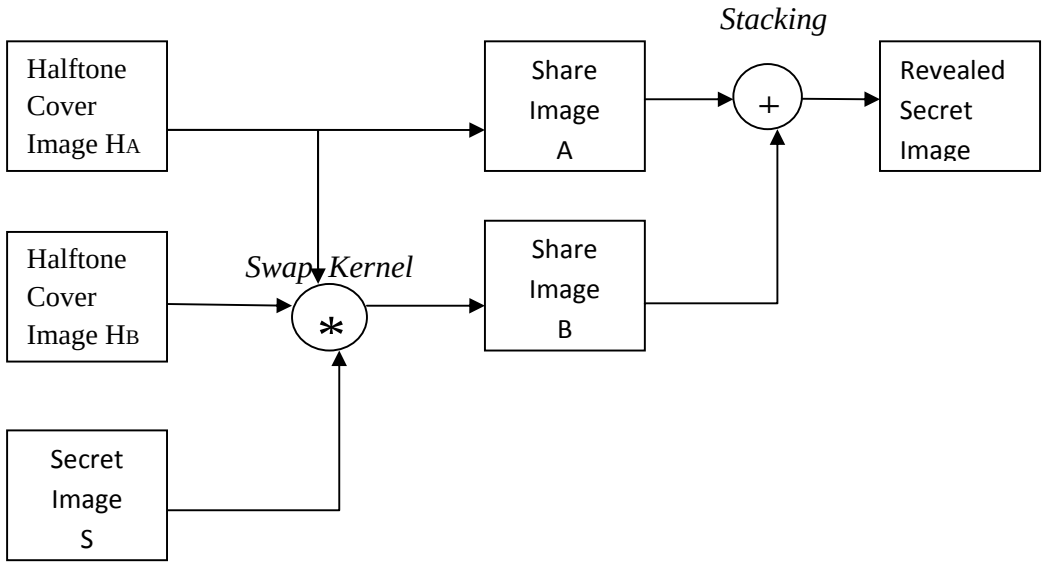


Fig 2. Block diagram of Chang et al's model [2]

III. RELATED WORKS

1. A. A Error Diffusion Halftone Technique

Before diffusing the secret image into the input images it is necessary to convert the two input images, one secret image and one extra confidential image into halftone equivalent. Halftonning is the pixel representation in the space each pixel may vary in their size, shape and the distance between the pixels. Hence the half toning process represents the different grayscale with the denser appearance of the black pixels. The density of the black pixels in a particular area represents the low degree of grayscale. The sparser of the black pixels in a particular area represents the high degree of grayscale. For half toning, Floyd Steinberg dithering process is used. Here each pixel has been visited and checked with threshold value then distribute the errors to its neighboring pixels that should have not been visited yet. Floyd Steinberg diffusion matrix of distributing the quantification residuals can be distributed to the four neighboring pixels shown in Fig.3 and Floyd–Steinberg dithering process flow chart is given in Fig.4.

The Floyd Steinberg dithering process can be described by the following equations (1) and (2) here 128 is the threshold value for all the pixels.

$$Q(u_{i\,.j}) = \begin{cases} 255\ (white\ pixel\ color), u_{i,j} \geq 128 \\ 0\ (black\ pixel\ color), u_{i,j} < 128 \end{cases} \quad (1)$$

$$e_{i,j} = \begin{cases} u_{i,j} - 255, u_{i,j} \geq 128 \\ u_{i.j}, u_{i,j} < 128 \end{cases} \quad (2)$$

Where,

$e_{i,j}$ is the quantified error at location (i, j),

and $Q(u_{i\,.j})$ is used to determine a pixel value to be 0 or 255,

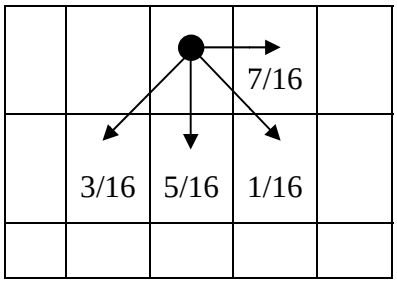


Fig 3. Floyd Steinberg diffusion matrix of distributing the error to neighboring pixels.[1]

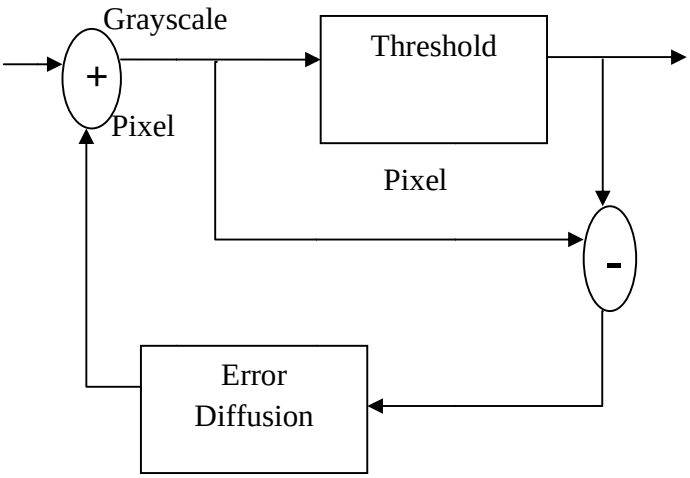
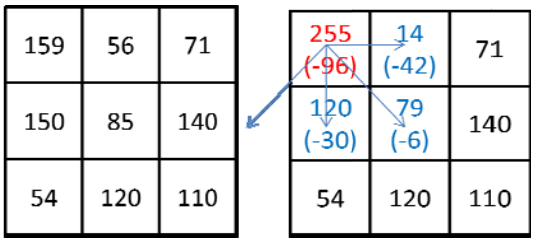


Fig. 4. Flow chart of the Floyd–Steinberg dithering process.[1]

Following is an example for converting the input image to halftone pixel. As already discussed the threshold value taken is 128.From the figure (Fig 5) each pixel is processed, take the first pixel which is 159, it should be compared with the threshold value. Hence it is ≥128 , replace 255 as halftone value in the place of 159, then evaluate the error residual by subtracting the value 159 by 255 according to equation (2) .

The resultant is -96, now distribute the residual to the neighborhood pixel by the matrix given in fig.3. 7/16 of the fractional to the right next pixel,1/16 of the fractional to the right down diagonal,5/16 to its down pixel and 3/16 to its left down diagonal. Repeat the process to meet or visit all the pixels in the matrix. The distribution of error differs in each row and each column. For eg., the first pixel residual distributed to three neighboring pixels. The second pixel residual distributed to four pixels. The third pixel residual distributed to the two neighboring pixels and so on till every pixel is met, see fig.3. Example is discussed in the fig.5.



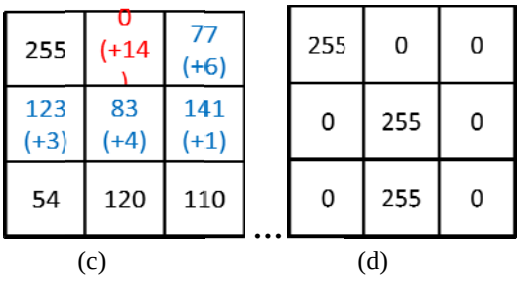


Fig. 5 Floyd's Steinberg Dithering process an example [1](a) Image represented in pixel (b) resultant after visiting the first pixel (c) resultant after visiting the second pixels(d) resultant after meeting all the pixels.[1]

IV. PROPOSED SYSTEM

In this proposed system, the input cover images and output share images are halftone images. Halftone images represent the property of the images by varying the density of black pixels. Each Pixel in the multi tone image is converted to binary image with only black and white pixel.

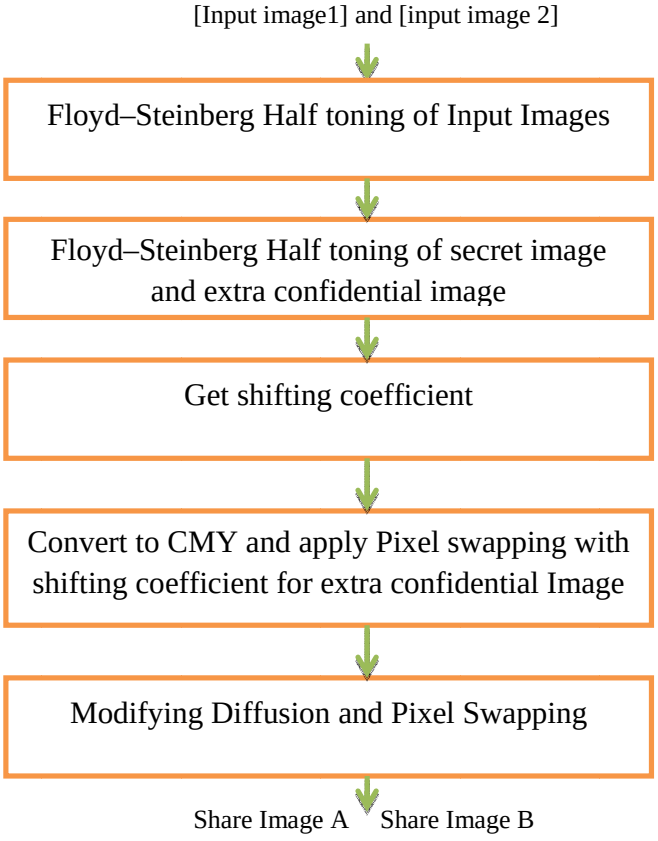


Fig.6 Embedding Phase of the Shifting Coefficient Method

Half toning reduces the size of the original image and also retains the image quality. The multi toned input image should also be converted into half toned by using the error diffusion technique.

The two input images, secret image and the extra confidential image are converted into halftone image, while converting the extra confidential image it is necessary to give the shifting co efficient value to obtain the extra confidential image. Because revealing secret image is simply stacking both the share images together whereas for revealing the extra confidential image, the first share image has to be placed constant and the second share has to be shifted to certain units.

Thus that certain unit is given as a value in shifting coefficient technique. After getting the shifting coefficient value the algorithm shifts the second share to N/2 units in addition to the shifting coefficient value. Further the pixel has been swapped to diffuse the secret image and the complete process is depicted clearly in the fig.6.

2. *A. Shifting Coefficient*

After converting input image A, input image B, secret image to the halftone technique the extra confidential image has to convert and then undergo the process of pixel swapping by getting the shifting coefficient value. This shifting coefficient value is like a key unless the receiver gets this key value from the sender, cannot recover the extra confidential image. Hence the shifting coefficient value is maintained as secret to avoid unauthorized attacks.

3. *B. Stacking*

Stacking is the process of superimposing one image on another image. If the two share images have been kept separately, no secret image can be revealed to the participant or the receiver. Whereas by stacking both the share images, thus the secret image can be revealed to the participant or receiver. With no additional computation has been made. The secret image can be viewed in human visual system and not decrypted separately by any tools. Also by keeping the one share fixed and shifting the other share to right by using the shifting coefficient value thus the extra confidential data which holds the lifetime of the message also promotes the authentication has been revealed to the participant or receiver.The extraction phase of the Shifting Coefficient Method is illustrated as a flow diagram in fig.7.

4. *C. Advantage*

This shifting coefficient act as a key for encrypting and decrypting the share images, hence without knowing the Shifting coefficient key value the extra confidential image cannot be recovered. Therefore it provides high security in recovering the extra confidential data for authentication.

Share Image A Share Image B

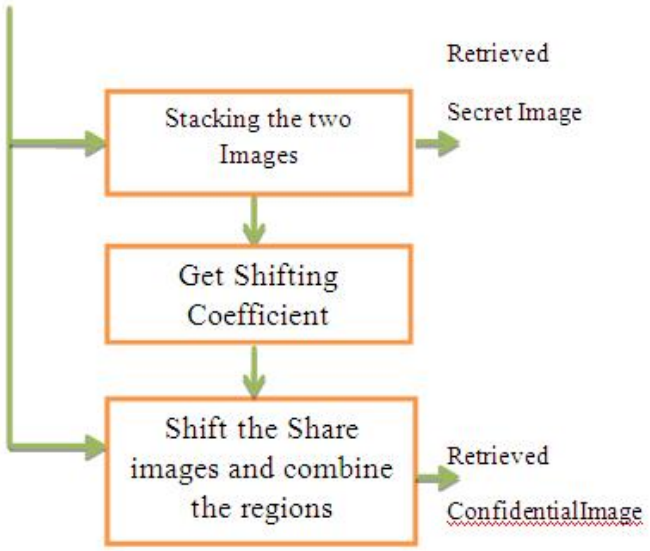


Fig 7. Extraction phase of the Shifting Coefficient Method

V. PERFORMANCE PARAMETER

To evaluate the performance of the proposed system, it is necessary to calculate the accurate rate of images used in this system (i.e.) the accurate rates of stacking result of original cover images and share images generated by the algorithm. The accurate rates of black secret area and white secret area are represented as AR_B and AR_W which can be obtained by the following equations (3) and (4).

$$AR_B = \frac{|SR=SI=0|}{|SI=0|} \quad (3)$$

$$AR_w = \frac{|SR=SI=1|}{|SI=0|} \quad (4)$$

Where SR represents the stacking result of share images, SI represents secret image, symbol '0' (zero) denotes black pixels and symbol '1' (one) denotes the white pixels. For white secret region, this method converts the stacking result to as white as possible in order to increase the revealing contrast. On the other side, for the black secret region, this method converts the stacking result to as black as possible in order to increase the accurate. Hence, the difference between the white secret region and the black secret region is observed.

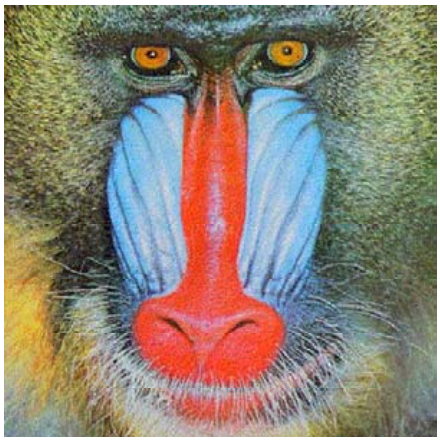
VI. RESULTS AND DISCUSSIONS

The following is the experimental results obtained from the proposed method of Visual Secret Sharing Scheme. fig.8 is the basic input images Baboon and Lena which are ready to be processed. Fig.9 holds the Half toned images of Baboon and Lena. The Secret image holds the secret message of "meet me at Richie park" fig .10 (a) and Extra Confidential Image holds the name "John" fig 10(b).Finally the fig.11are the share images which are to be sent to the receiver or participant. Fig.12.(a) is the Revealed Secret Image and Revealed Extra Confidential Image by Shifting Coefficient is obtained fig 12(b).

(a)

(b)

Fig.8. Iinput images (a) Baboon (b)Lena

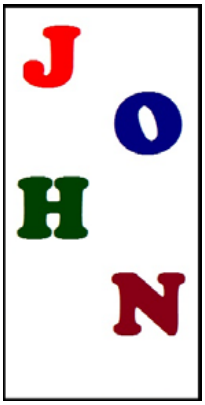


(a)

(b)

Fig.9. Halftoned Images (a) Baboon (b)Lena

(a)



(b)

Fig.10. Images (a) Secret Image (b) Extra Confidential Image

(a)

(b)

Fig.11. Share Images (a) Baboon (b) Lena

(a) (b)

Fig.12. Images (a) Revealed Secret Image (b) Revealed Extra Confidential Image by Shifting Coefficient

The accurate rate of the different main secret images and extra confidential images are calculated by the formula given in equation (4) and (5) and its result is given separately for the black pixels and white pixels as well called the ARb and ARw for four different set of secret images and extra confidential images in the following Table I. and its corresponding graphical representation for four trials is given in the fig. 13.depicts the accurate rate for black and white pixels for different secret images and extra confidential images.

TABLE I . ACCURATE RATE OF THE DIFFERENT SECRETS IMAGE AND EXTRA CONFIDENTIAL IMAGES

	ARB	ARw
Main Secret 1	0.8912	0.6934
Extra Confidential 1	0.8722	0.3155
Main Secret 2	0.9065	0.7219
Extra Confidential 2	0.9041	0.3388
Main Secret 3	0.9076	0.8495
Extra Confidential 3	0.8719	0.3865
Main Secret 4	0.9139	0.8634
Extra Confidential 4	0.8890	0.3989

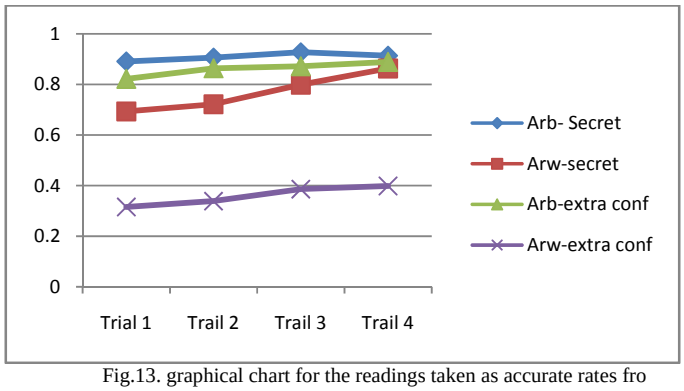


Fig.13. graphical chart for the readings taken as accurate rates fro the experiment (table I)

VII. CONCLUSION

This paper generates a secure color visual secret sharing scheme in which a secret image has been hidden into two other meaningful cover images without the pixel expansion and also embeds an extra confidential data for authentication by using the shifting coefficient method in order to provide more security. The receiver or participant who receives the two share images can place one on another image to reveal the secret image and to reveal the extra confidential image the shifting coefficient is needed to shift it with N/2 units. Unless the receiver is aware of the shifting coefficient cannot reveal the extra confidential image. Thus this method provides more security with key like structure in transmitting of the images across internet.

REFERENCES

[1] Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, Chwei-Shyong Tsai, "A novel authenticable color visual secret sharing scheme using non expanded meaningful shares", Elsevier on Displays,vol.32,pp.118-134,2011

[2] Y.-F.Chang,J.-B.Feng,,C.-S.Tsai,Y.-P.Chu,H.C.Syu, "New data hiding scheme using pixel swapping halftone images" The Imaging Science Journal, vol 56,pp no.279 -290, 2008.

[3] H.C. Wu, H.C. Wang, R.W. Yu, "Color visual cryptography scheme using meaningful shares", *Eighth International Conference on Intelligent System Design and Applications* vol. 3 pp. 173–178, 2008.

[4] S.J. Shyu," Image encryption by random grids", *Pattern Recognition* vol .40 no.3 pp.1014–1031, 2007

[5] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen c, Yao-Te Huang " A novel secret image sharing scheme for true-color images with size constraint" *Information Sciences* vol. 179 pp. 3247–3254,2009.

1. M.John Justin received the B.E degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2010,and pursuing his M.Tech degree in Software Engineering in Karunya University, Coimbatore ,India .His research interests include image processing, software engineering.

2. S.Manimurugan received the B.E. degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2005, and the M.E. degree in Computer Science and Engineering in 2007. He is currently pursuing the Ph.D. degree in Computer Science and Engineering in Anna University, Coimbatore, India. His current research interests are in Image Processing, Information Security.

3. B.Alagendran received the B.E degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2010, and pursuing his M.Tech degree in Software Engineering in Karunya University, Coimbatore, India. His research interests include image processing, software engineering, data mining.