International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:8, 2015

# Threshold Based Region Incrementing Secret Sharing Scheme for Color Images

P. Mohamed Fathimal, P. Arockia Jansi Rani

***Abstract*—**In this era of online communication, which transacts data in 0s and 1s, confidentiality is a priced commodity. Ensuring safe transmission of encrypted data and their uncorrupted recovery is a matter of prime concern. Among the several techniques for secure sharing of images, this paper proposes a k out of n region incrementing image sharing scheme for color images. The highlight of this scheme is the use of simple Boolean and arithmetic operations for generating shares and the Lagrange interpolation polynomial for authenticating shares. Additionally, this scheme addresses problems faced by existing algorithms such as color reversal and pixel expansion. This paper regenerates the original secret image whereas the existing systems regenerates only the half toned secret image.

***Keywords*—**Threshold Secret Sharing Scheme, Access Control, Steganography, Authentication, Secret Image Sharing, XOR, Pixel Expansion.

## I. Introduction

IN the recent years of ecommerce, most computing activities are moved from a peer-to-peer computing environment to a centralized client-server environment. With the growth of cloud computing environment, all industries are outsourcing their electronic databases to storage centers. It has become a common practice to process all documents (text, images and multimedia), store securely in a data center for future access, and share over the internet. Users store and work in such centers with little knowledge of their internal structure. Single-point storage poses the danger of data loss as well as issues of privacy. From the user's perspective, achieving confidentiality, integrity and availability of storage in the cloud is a serious issue. Secret sharing scheme is a cryptographic method that shall address both integrity and availability issues simultaneously.

A *(k, n)* threshold secret sharing scheme is a cryptographic technique designed to distribute a secret S for n participants in such a way that a set of k or more participants can recover the secret S, and a set of k-1or fewer participants cannot obtain any information about S. In this traditional visual cryptography scheme, the secret is a single image and the scheme applies same encoding rule for all pixels in that image. Therefore, it reveals either the entire image or nothing. Many applications require sharing multiple secrets in which number of secrets revealed is proportional to the number of participants engaged in the decoding process. The region incrementing visual cryptographic scheme (RIVCS) divides a single image into different regions based on secrecy level and applies different encoding rules to each of these regions. In recovery process, stacking $j+1$ shares decodes j-th level regions.

This paper presents a *k* out of *n* region incrementing scheme in which the dealer can split the content of the secret color image into *n–k* equal regions and assign a secrecy property to each region. Each share looks like a random image and by stacking *k* number of shares reveals the first secrecy region. Stacking more and more shares reveals the entire secret image.

The organization of the rest of this paper is as follows. Section II discusses the related literature. Section III discusses the proposed scheme. Section IV analyses the experimental results. Finally, Section V concludes the paper.

## II. Related Literature Review

There are two main categories of secret image sharing scheme: One based on the visual cryptography and the other based on Lagrange's Polynomial Interpolation.

The visual cryptography introduced by Naor and Shamir [1] shares visual information (pictures, text, etc.) in an encrypted form so that the participants can restore the secret without the aid of a computing device. The design is restricted to only binary images and some additional processing such as half-toning and color-separation are required for color images. The superposition of two shares is tedious for high-resolution images and this scheme can recover only half toned secret image with the loss of resolution.

The Polynomial-based secret image sharing proposed by [2] and [3] is to hide secret pixels as constant terms in $(k-1)$ degree polynomials using Lagrange Interpolation. An Interpolating function for a set of data $\{(x_1, y_1), (x_2, y_2) \ldots (x_n, y_n)\}$ is a function $f(x)$ that satisfies: $f(x_1) = y_1, \ldots.. f(x_n) = y_n$.

In [2], there are *n* participants and a mutually trusted dealer. Let *p* be a large prime and GF (*p*) denote Galois Field of order *p*. The scheme consists of two phases— Partitioning Phase and Regeneration Phase. In the Partitioning phase, the dealer constructs a *(k-1)* - degree polynomial

$$y = f(x) = (a_0 + a_1x + .. a_{k-1}x^{k-1}) mod\ z$$

P. Mohamed Fathimal is with the Manonmaniam Sundaranar University, Tamil Nadu, India (phone: 9943897935; e-mail: fatnazir@gmail.com).

P. Arockia Jansi Rani is with Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tamil Nadu, India (e-mail: jansi_cse@msuniv.ac.in)

where $a_1 \ldots a_{k-1}$ are randomly chosen from GF ($p$), and $a_0 = f(0) = s$ is the shared secret and computes $s_i = f(x_i) \bmod p$ for $i = 1, 2 \ldots n$. The dealer distributes the shares are then distributed to the corresponding participants over a secure channel. In the Regeneration Phase, with the knowledge of $k$ pairs of ($x_i$, s (i)), the dealer determines the $(k-1)$-degree polynomial $f(x)$ using the Lagrange interpolation polynomial as:

$$s(i) = f(0) = \prod_{j=1\, j!=i}^{k} \frac{(-x_i)}{(x_i - x_j)} mod\ p \qquad (1)$$

By solving this polynomial for each pixel value, the authorized participants can restore the original host image from the shadow images. The following section discusses (k, n) region incrementing schemes developed by some researchers.

Reference [4] developed a region incrementing visual cryptographic scheme in which the secrets in the original image are hidden in such a way that each level of the secrets is obtained by stacking more number of the shares in the decoding process. The main disadvantage of this scheme is it generates noise like share images and it requires a preprocessing technique like half-toning to convert color image into bi-level image. Further, the certain colors of the reconstructed image are reversed.

Reference [5] developed a systematic construction of (*2, n*) RIVCS in which the appeared colors are correct for all regions but it suffers from pixel expansion problem.

Reference [6] proposed a modified (*k, n*) scheme to reduce the shadow size and to increase the contrast. This scheme also has the problem of color reversal in some secrecy level. So this scheme is best suited for applications where secret image is a bi-level image and the shape or text of the image is necessary than the color of the secret. All the above mentioned schemes converts color image into bi-level image using half toning technique and recovers only the half toned secret image.

The proposed scheme overcomes the above-mentioned problems like color reversal, pixel expansion and low contrast. This scheme processes color image directly, thus eliminates the need for half-toning process and recovers the original secret image without any loss.

## III. Proposed Work

This section describes the proposed region incrementing secret sharing scheme in detail. The scheme consists of two processes- Sharing and Recovery. Sharing Process has two phases namely the Initialization Phase and Key Generation and Partitioning Phase. The Recovery Process has two phases- Regeneration and verification and Post Processing.

### *A. Sharing Process*

1. Initialization Phase

This phase involves generation and assignment of unique key value for each participant in the dealer side. The dealer then distributes the unique key *(x, f(x))* for each participant to validate his or her shares. This helps to avoid fabrication of shares by the hackers. The hackers or dishonest participants cannot fabricate share recovery unless they provide the correct unique key value *(x, f(x))*.

Reference [2] secret sharing scheme uses the Lagrange interpolation polynomial for every pixel in the secret image. This paper employs the Lagrange interpolation polynomial for generating authentication key.

The unique authentication key generation procedure is given below:

Step 1: Consider the polynomial $f(x) = (a_0 + a_1x + a_2x^2 \ldots + a_{k-1}x^{k-1}) \bmod z$ where the coefficients $a_0\ a_{1\ldots}\ a_{k-1}$ are random numbers in the range of [1, 255].

Step 2: Compute the unique authentication id $y(x) = (x, f(x))$ *where* $x \neq 0$ i.e. $y(1)=(1,f(1)), y(2)=(2,f(2)) \ldots y(n)=(n, f(n))$. This unique authentication id is a pair of two integers. If any *k-1* of *n* participants gathers, then they can reconstruct the coefficients.

2. Key Generation and Partitioning Phase

This phase describes the procedure of sharing the image $I$ among n participants such that the combination of unique $k$ shares from $k$ participants shall generate the first secret image section without distortion.

Given a secret image $I$ of size $r \times c \times d$, the dealer splits the content to $t$ equal sections. The number of regions or sections in an image ($t$) is $t=n-k$. The secret image I and the key image are block matrices containing t sections or blocks namely $I_1, I_2, I_3, I_4$ and $key_1, key_2\ key_3, key_4$ respectively. A block matrix is a matrix whose elements are matrix themselves. For example, if t=4 ($t=n-k$), then the image is divided into sections namely $I_1, I_2, I_3 and I_4$. The secret Image

$$I = \begin{bmatrix} I_1 & I_2 \\ I_3 & I_4 \end{bmatrix}$$

and key image *key* is

$$key = \begin{bmatrix} key_1 & key_2 \\ key_3 & key_4 \end{bmatrix}$$

Algorithm 1 generates the participant shares and key image of size r × c × d. The first section of the image is assigned to $x_1$ . $XOR$ the $i_{th}$ sections of the image with $x_{i-1}$ to generate $x_i$ for all i = 2 …t. The output $x_t$ is divided by $k$ and the remainder pixel values (*modulo k*) obtained. XOR the difference of $x_t$ $and\ its\ modulo\ 255$ with $x_t$ to obtain $z$. The difference of $x_t$ $and\ its\ modulo\ 255$ is divided by $k$ $to$ generate R. This helps to avoid loss of data occurred during integer division.

XOR the image sections $I_2, I_3, \ldots. I_t$ $and\ R$ to obtain the first section of the key image ( $key_1$). XOR $x_i$ $and\ R$ to obtain $key_i$ of key image where i =2… t. Then, right-shift the R-value circularly by $d_x$ times. The value $d_x$ is obtained by multiplying participant number $x$ and the coefficient $a_{x mod\ k-1}$ (used in the initialization phase) to generate $S_x$. Similarly, key sections generated are circularly right shifted by constant terms obtained by solving *k, (k+1), (k+2) and (k+3)* combinations of *(x, f (x))*.

*Algorithm 1:*
*Input:*
a. *Number of Shares n,*

b. *Number of sections t,*
c. *Number of shares required to recover the shares k,*
d. *Secret Image I of size r× c× d ,*
e. *Set of n unique ids y (1)….y (n) (for each participant) and coefficients $a_0$ $a_1$… $a_{k-1}$ of polynomial f(x).*

*Output:*

*N shares $S_1 \dots S_n$ of size r/2× c/2×d*

*Step1: Split the image I into n-k sections $I_1$,$I_2$, $I_3$ and $I_4$.*

*Step 2: Generate Share images $Sr_1 \dots\dots Sr_k$ and key image key as follows*

$$x_1 = I_1 \text{ for i=1,}$$

$$x_i = x_{i-1} \oplus I_i; \text{ for all i= 2, 3. …t,}$$

$$z = x_t \oplus (x_t - x_t \bmod k)$$

*Step 3*: T*he image $x_t$ is then subtracted from z. The resultant matrix is then divided by k (threshold number of shares) to produce R.*

$$R = (x_t - x_t \bmod k)/(k)$$

$$key_1 = I_2 \oplus I_3 \dots\dots \oplus I_t \oplus z \text{ for i=1}$$

$$key_i = x_i \oplus R \text{ for all i=2,3,…t}$$

*Step 4: In order to aid authentication and to avoid fabrication of shares, the image R is left shifted circularly by $d_x$ times to generate the share for each participant.*

$$d_x = (a_{x \bmod k} * x) \bmod 255$$

$$S_x = rightcircularshift\,(R, d_x)$$

*where 1 ≤ x ≤ n*

*Step 5: The constant term for k-1 degree polynomial f(x) = ($a_0$ +$a_1x$ +$a_2x^2$ …+$a_{k-1}$ $x^{k-1}$) mod z is $a_0$ and is assigned to $y_1$.Similarly using (k+1), (k+2) and (k+ t) combinations of (x, f(x)), solve the polynomial of degree k, (k+1) and (k+t-1). The constant term of these polynomials are assigned to $y_x$ for all x=2...t.*
*Right shift the key circularly by $b_x$ times.*

$$b_x = (y_x) \bmod 255$$

$$key_{x1} = rightcircularshift\,(key_x, b_x)$$

*for all x= 1…t;*

*Step 6: This share image $S_x$ and the authentication id y(x) =(x, f(x)) where 1 ≤ x ≥ n is distributed to each of n participants. The key image key of size r× c× d is generated as a block matrix using the keys $key_x$ where 1 ≤ x ≤ t.*

### *B. Recovery Process*

The recovery process has two phases.

1. Regeneration and Authentication Phase

In this phase, *Algorithm2* describes the recovery of first section of the original image. XOR the sum of shares $Srec_x$ from *k* participants and $key_{11}$ to recover the first section of the image. Step 2 solves the polynomial *f(x)* to find the coefficients using the authentication id (*x, f(x))* of the *k* participants. Each share $Srec_x$ is left-shifted circularly by the resultant of coefficient multiplied by *x mod 255* to calculate $Sr_x$ *in Step3. It* then checks whether all the k shares $Sr_x$ are equal. This condition assures that the share images are free from modification. If all the shares are equal, the $key_{11}$ from the database is then left- shifted circularly by $a_0$ and stored in $kr_1$.Then, the participants' shares $Sr_1 \dots\dots Sr_k$ are added and XOR- ed with $kr_1$ to recover the first section $Rr_1$.

To retrieve the remaining sections $Rr_1, Rr_2 \dots Rr_t$ of the secret image *I*, solve the *k, k+1 and k+t-1* degree polynomial f(x) to determine the coefficients $a_{10}, a_{20}$ *and* $a_{30}$ using *k, k+1, k+2…k+ t* pairs of *(x, f(x)).*

*Algorithm 2:*
*Input:*

1. *k number of participant images of size r/2×c/2×d,*
2. *set of k unique ids y (1)….y (k) (for each participant)*
3. *Key image and*
4. *Total Number of participants (n) from the database*

*Output: Sections of the Secret Image $Rr_1, \dots\dots Rr_4$ of size r/2×c/2×d*

*Step1: Let the share images of k participants be $Srec_x$ where 1 ≤ x ≤ k. Calculate number of regions or sections in the secret image t= n-k.*

*Step 2: With the knowledge of k pairs of (x, f(x)), determine the (k-1) degree polynomial f(x) and the coefficients are calculated using the following equation.*

$$s = f(0) = \prod_{j=1 j!=i}^{k} \frac{(-xi)}{(xi-xj)} \bmod p$$

*Step 3: Authenticate shares and check the integrity of the cover image by calculating*

$$dr_x = (a_{x \bmod k-1} * x) \bmod 255$$

$$Sr_x = leftcircularshift\,(Srec_x, dr_x)$$

*where 1 ≤ x ≥ k.*

*if $Srec_1 == Srec_2 = \cdots . Srec_k$ the shares are not modified and share from database can be accessed.*

$$w_1 = (a_0) \bmod 255$$

$$kr_1 = leftcircularshift\,(key_{11}, w_1)$$

*Step 4: calculate $Rr_1$*

$$Rr_1 = kr_1 \oplus (Sr_1 + Sr_2 \dots + Sr_k)$$

*Step 5: $Rr_1$ is the first section of the image $I_1$ and the size of $Rr_1$ is r/2× c/2×d. To retrieve section$Rr_2$, determine the k -degree polynomial f(x) using the k+1 pairs of (x, f(x)). The constant term modulus 255 ($w_2$) calculated.*

$$kr_2 = leftcircularshift\,(key_{21}, w_2)$$

$$Rr_2 = Rr_1 \oplus kr_2 \oplus Sr_{k+1}$$

*Step 6: Similarly to retrieve the remaining sections $Rr_i$ where i= 3… t, the k +i pairs of (x, f(x)) are used to solve the (k +i-1) degree polynomial f(x) and the constant $w_i$ is calculated.*

$$w_1 = (a_0) \bmod 255$$

$$kr_i = leftcircularshift\,(key_{i1}, w_i)$$

$$Rr_i = Rr_1 \oplus Rr_2 \oplus Rr_3 \ldots\ldots \oplus kr_i \oplus Sr_{k+i-1}$$

2. Post Processing

Generate a block matrix $R$ using $Rr_1, Rr_2, Rr_3 \ldots\ldots Rr_t$. All these t elements are in the size $r/2\times c/2\times d$ and the matrix $R$ is of size $r\times c\times d$.

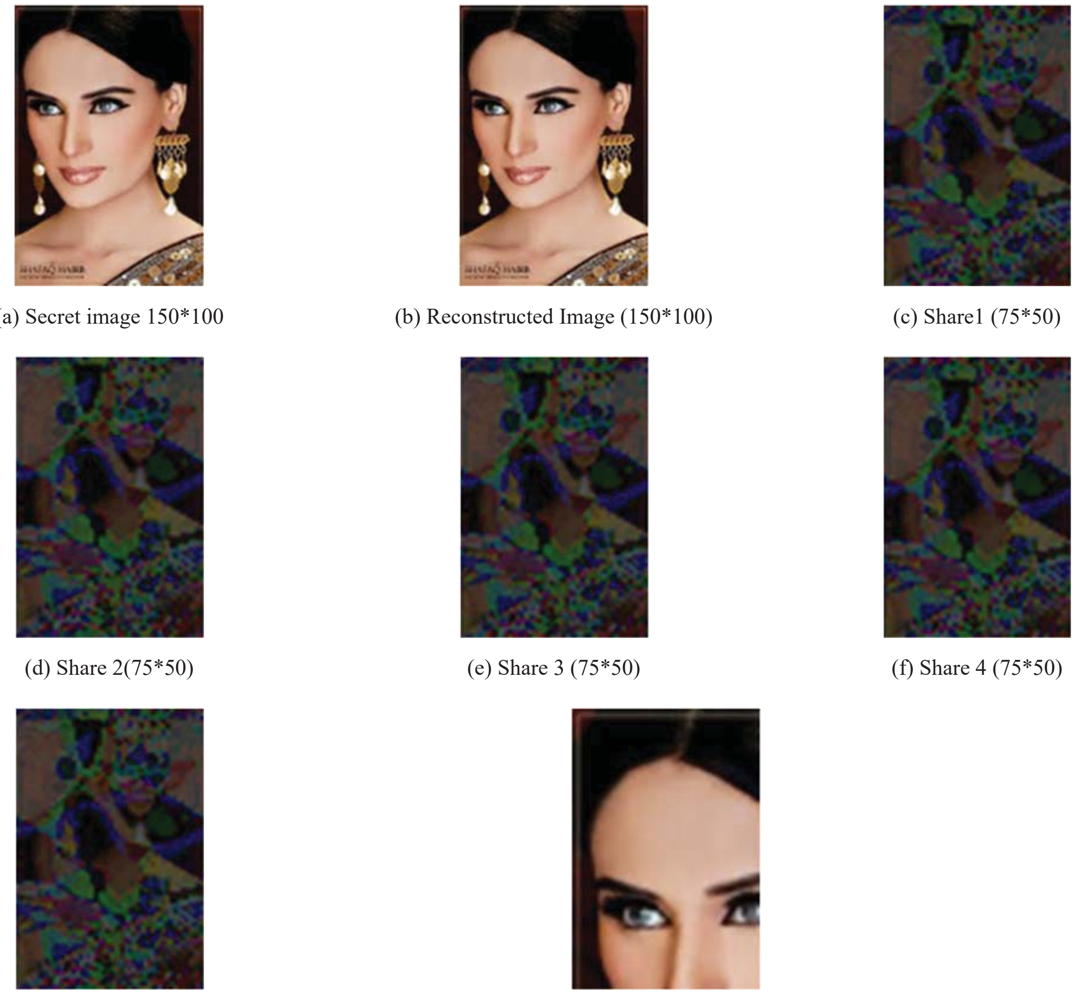
$$R=\begin{bmatrix} Rr_1 & Rr_{t/2} \\ Rr_{t/_2+1} & \ldots Rr_t \end{bmatrix}$$

Thus, this scheme recovers the secret image without any loss.

## IV. Experimental Results and Analysis

In this section, the experimental results show the feasibility of the proposed scheme. The method described in this paper is implemented in *Matlab 10.0* running on *Windows 8.* Experiments performed on *i5 Processor* with *4 GB* of memory.

To test the visual quality of the image, the secret image is *img1* with size *150*150*. The values set for *k* is *3* and *n* is *5.* So for this *(3, 5)* proposed sharing scheme, the output is shown in Fig. 1.



(a) Secret image 150*100 (b) Reconstructed Image (150*100) (c) Share1 (75*50)

(d) Share 2(75*50) (e) Share 3 (75*50) (f) Share 4 (75*50)

(g) Share 5 (75*50) (h) First Region of the Image after combining k=2 shares and key1

Fig. 1 Experimental Results for (3, 5) proposed scheme with their PSNR

The criteria for the visual quality of the image is the peak signal to noise ratio which is defined as

$$MSE = \frac{1}{mn}\sum_1^m \sum_1^n [\, I_{ij} - I'_{ij}]^2 \tag{2}$$

$$PSNR = 20 * log_{10}(max_f\ / sqrt(MSE)) \tag{3}$$

where $I$- Original image of size $m \times n$, $I'$-Recovered image of size $m \times n$ and $max_f$ - Maximum intensity value that exists in the original image (255).

The higher the PSNR value, better the quality of the reconstructed image [7]-[12].

The pixel expansions of the proposed (k, n) RIVCS, Wang's scheme [4], Yang's scheme [5] and Yang's modified scheme [6] are given in Table I. It is observed that the proposed scheme has share image size less than the original secret image when compared to other schemes which has pixel expansion greater than 4.

Table II depicts the comparison of contrasts of the proposed scheme with the existing schemes. It shows that the proposed scheme shows the better contrast in all secrecy levels when comparing to other schemes.

TABLE I
COMPARISON OF PIXEL EXPANSION FOR THE PROPOSED (K, N) SCHEME WITH THE EXISTING SCHEMES

| (k, n) RIVCS | Reference [4] | Reference [5] | Reference [6] | Proposed Scheme |
|---|---|---|---|---|
| k=2,n=3 | 4 | 6 | 4 | 1/n-k |
| k=2,n=4 | 10 | 18 | 10 | 1/n-k |
| k=2,n=5 | 20 | 44 | 23 | 1/n-k |

TABLE II
COMPARISON OF CONTRAST OF THE PROPOSED SCHEME WITH THE EXISTING SCHEME

| (2,5) RIVCS | Security Level | | Reference[4] | Reference[6] | Proposed Scheme |
|---|---|---|---|---|---|
| K=2 | 1st | Stacking 2 shares | 4/23 | 1/5 | 1 |
| | | Stacking 3 Shares | 6/23 | 3/10 | 1 |
| | | Stacking 4 shares | 7/23 | 7/20 | 1 |
| | | Stacking 5 shares | 7/23 | 7/20 | 1 |
| K=2 | 2nd | Stacking 2 shares | - | - | - |
| | | Stacking 3 Shares | 1/23 | 1/20 | 1 |
| | | Stacking 4 shares | 3/23 | 1/10 | 1 |
| | | Stacking 5 shares | 6/23 | 3/20 | 1 |
| K=2 | 3rd | Stacking 2 shares | - | - | - |
| | | Stacking 3 Shares | - | - | - |
| | | Stacking 4 shares | 1/23 | 1/20 | 1 |
| | | Stacking 5 shares | 3/23 | 3/20 | 1 |
| K=2 | 4th | Stacking 2 shares | - | - | - |
| | | Stacking 3 Shares | - | - | - |
| | | Stacking 4 shares | - | - | - |
| | | Stacking 5 shares | 1/23 | 1/20 | 1 |

## V. CONCLUSION

This paper presents a threshold region incrementing color image-sharing scheme, which generates the meaningless shares with size lesser than the secret images and thus eliminating pixel expansion. This scheme uses simple arithmetic and Boolean operations and hence the computational complexity is *O (n)*). Experimental results show that the visual quality of the recovered image has better PSNR (infinity) when compared to the other existing schemes. This scheme prevents fake share images and thus ensures authentication. This scheme can further be enhanced with the sharing of multiple secret images.

## REFERENCES

[1] N. Noar, A. Shamir, 1995. "Visual Cryptography", Advances in Cryptology: Eurocrypt' 94, Vol. 48, Springer, Berlin, 1995, Pp.1–12.
[2] A. Shamir, 1979. How to Share a Secret. Commun. Acm 22 (11), 612–613.
[3] G. R. Blakley, 1979. "Safeguarding Cryptographic Keys". In: Proc. Fips National Comput. Conf. 48, 313–317.
[4] Ran-Zang Wang. "Region Incrementing Visual Cryptography." IEEE Signal Processing Letters (2009): 659-662.
[5] Yang, Ching-Nung, Hsiang -Wen Shih and Yu-Ying Chu and Lein Harn. "New Region Incrementing Visual Cryptographic Scheme."
[6] Ching-Nung Yang, Hsiang -Wen Shih, Chih-Cheng Wu and Lein Harn. "k out of n Region Incrementing Scheme in Visual Cryptography." IEEE Transactions on Circuits and Systems for Video Technology (2012): 799-810.
[7] P. Mohamed Fathimal, P. Arockia Jansi Rani, "K out of N Secret Sharing Scheme for Gray and Color Images", IEEE International Conference on Electrical, Computer and Communication Technologies, March 2015.
[8] P. Mohamed Fathimal, P. Arockia Jansi Rani, "Bidirectional Serpentine Scan Based Error Diffusion Technique for Color Image Visual Cryptography", International Journal of Science, Engineering and Technology Research, 2014.
[9] P. Mohamed Fathimal, P. Arockia Jansi Rani, "(N, N) Secret Color Image Sharing Scheme with Dynamic Group", International Journal of Computer Network and Information Security, June, 2015.
[10] P. Mohamed Fathimal, P. Arockia Jansi Rani, "Design of Block based Visual Secret sharing scheme for color Images", International Journal of Applied Engineering Research, May 2015.
[11] Mohamed Fathimal P., P. Arockia Jansi Rani, "K out of N Secret Sharing Scheme with Steganography and Authentication", Advances in Intelligent Systems and Computing, Springer 2015.
[12] Mohamed Fathimal P, P. Arockia Jansi Rani, "K out of N Secret Sharing Scheme for Multiple Color Images with Steganography and Authentication", International Journal of Imaging and Graphics (Accepted), (2015).

**P. Mohamed Fathimal** received her BE and ME in Computer Science and Engineering from Manonmanium Sundaranar University, Tirunelveli, Tamilnadu. She has 10 years of Teaching Experience. Currently she is pursuing PhD in Manonmanium Sundaranar University. Her research interests include Digital Image Processing and Information Security.

**Dr. P. Arockia Jansi Rani** graduated B.E in Electronics and Communication Engineering from Government College of Engineering, Tirunelveli, Tamil Nadu, India in 1996 and M.E in Computer Science and Engineering from National Engineering College, Kovilpatti, Tamil Nadu, India in 2002. She has been with the Department of Computer Science and Engineering, Manonmaniam Sundaranar University as Assistant Professor since 2003. She has more than ten years of teaching and research experience. She completed her Ph. D in Computer Science and Engineering from

Manonmaniam Sundaranar University, Tamil Nadu, India in 2012. Her research interests include Digital Image Processing, Neural Networks and Data Mining.