

Cumulative Image Encryption Approach

R. Das^{1*}, S. Dutta²

¹Development Officer, Bankura University, Bankura-722155, W.B., India.

²Department of Computer Applications, Dr. B. C. Roy Engineering College, Durgapur-713206, WB, India.

*Corresponding Author: ramkrishnadas9@gmail.com,, Tel.: +91-9647000821

Available online at: www.ijcseonline.org

Accepted: 19/May/2018, Published: 31/May/2018

Abstract—Secret sharing scheme divides colour image into user defined N (positive integer) number of shares with different transference where decryption is being carried out by human visual system using at least K (positive integer) number of shares out of N number of shares. In image key encryption technique the user perform user define BWM&AS operation (bit wise masking and alternate sequence) in between two constitutive bits of each pixel of original image and image key. In this combined approach we introduce two level of encryption using secret sharing scheme followed by Image key encryption technique using BWM&AS operation. Firstly, the original image is encrypted using an image key then that encrypted image is being divided into N number of shares where each of the share is again being encrypted by unique image key in encryption end. In decryption end, we retrieve original shares from the encrypted shares using appropriate image key and generate the original encrypted image by taking K number of share out of N. Lastly, we retrieve the original image by performing BWM&AS operation between the original image key and encrypted image. Thus an attempt is made to enhance the security.

Keywords— Secret Sharing, Human Visual System, Image Key Encryption Technique, BWM&AS Operation.

I. INTRODUCTION

Steganography is the practice and study of techniques for hiding the secured data within other data and it may be applied on image, audio file [9, 10]. A colour image consists of finite number of pixels where each pixel is being represented by 32 bits. Four groups each of 8 bits contain the information about transparency and red, green, blue colours [8]. Secret sharing scheme is a technique to divide a digital colour image into N number of shares each of different transparency where minimum K numbers ($N \geq k$) of shares are sufficient to reconstruct the image [7]. Encryption of one image by performing bit wise BWM&AS (Bit wise masking and alternate sequence) between the bit values of each pixel of original image and the image key is called image key based encryption technique [3, 4].

Here we have developed a procedure, where the original image is being encrypted using a user defined image key and followed by secret sharing scheme [7]. Thus produce N number of shares of the encrypted image. Now each of the shares being encrypted by the user defined image keys thus generate N numbers of encrypted shares. In decryption end, each encrypted share is being decrypted by the dedicated user defined image key and generates the

share of the encrypted image. Now we generate the original encrypted image by taking K number of share out of N. Lastly, we retrieve the original image by performing BWM&AS operation between the user defined image key and encrypted image. Most of the existing system used single level of encryption. We perform three level of encryption by performing image key encryption of original image, sharing of encrypted image and encrypting of each share. All the image keys and the number of share is being defined the user [3, 4]. Besides this most of the existing system used XOR operation where we have introduce new BWM&AS operation (bit wise masking and alternate sequence) which is a combination of multiple number of bitwise operation with proper sequence. Thus the system provides great security.

In this paper, section-II describes the background ideas; Section-III describes the overall procedure. Section-IV and section -V represent encryption and decryption procedure respectively. Experimental results are being described in section-VI and section-VII draws the conclusions.

II. BACKGROUND STUDY

In October 2015, Mohamad M. AL-Laham developed a novel encryption technique of RGB color image where

matrix multiplication is used. The original RGB color image matrix is multiplied with a random key matrix [1].

In 2014, Saksham Wason, Piyush Kumar and Shubham Rathi proposed a new technique where a variable length key is generated for text and image encryption depending on session type [2].

R. Das, S. Kulia and S. Dutta introduced a combined image encryption scheme in 2013 using Image Partitioning, Text Key Encryption, Image Key Encryption & Digital Enveloping techniques cumulatively on a color image. The schemes enhance the security as multilevel image encryption is performed here but the overhead is higher [3].

Again in 2013, A. Bhakta, S. Maity, R. Das and S. Dutta represent a multilevel Image Encryption Technique using Image-key encryption, Bit-Sieved operation and K-N secret sharing scheme which provide a great security with less overhead. Bit-Sieve operation has been introduced for the first time [4].

In 2012, S. Kandar and B.C Dhara introduce random sequence based secret sharing for color image which implemented a new technique for secret sharing [5].

S.M.M. Karim, Md.S. Rahman and Md. I. Hossain proposed LSB substitution method with secret key encryption in 2012 [6].

III. PLEMINARIES

A. Basic Color Concept:

A natural color digital image is composed of a finite number of elements called pixels. In a 32 bit digital image each pixel consists of 32 bits, which includes four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency A 32 bit pixel is represented in the figure 1 [8].

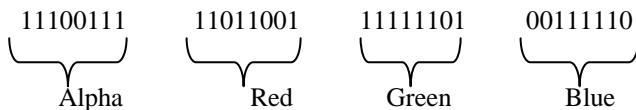


Figure 1. Structure of a 32 bit pixel.

B. Random number based Secret Sharing Scheme:

Here we have proposed an algorithm to divide a digital color image into n number of shares where minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining numbers of shares are (n-k). In an image if certain position of a pixel is 1, then in (n-k) +1 number of shares in that

position of that pixel there will be 1. In the remaining shares in that position of the pixel there will be 0. Those (n-k) +1 number of shares are selected using a random number generator [5].

C. Image key encryption technique:

Encryption of one image by performing bit wise BWM&AS (Bit wise masking and alternate sequence) between the bit values of each pixel of original image and the image key is called image key based encryption technique. Where size of the image key (p*q) must be less than or equal to the size of the original image (w*h). $p*q \leq w*h$ [3, 4].

D. BWM&AS Operation:

The Operation will be performed between the binary array representations of Original Image and Key Image. The procedure will follow the following rules:

Rule 1: For even bit position of Original Image

- a. If corresponding bit position value of Key Image = 0 then, Output = Corresponding bit value of Original Image.
- b. If corresponding bit position value of Key Image = 1 then, Output = Complement of corresponding bit value of Original Image.

Rule 2: For odd bit position of Original Image

- a. If corresponding bit position value of Key Image = 1 then, Output = Corresponding bit value of Original Image.
- b. If corresponding bit position value of Key Image = 0 then, Output = Complement of corresponding bit value of Original Image. Figure 2 represents BWM&AS operation.

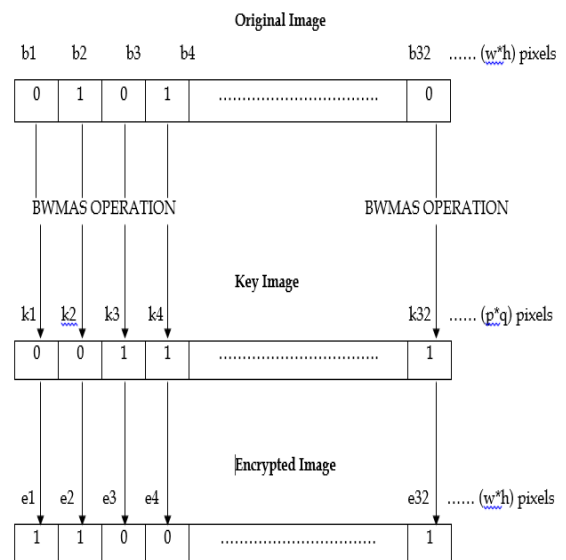
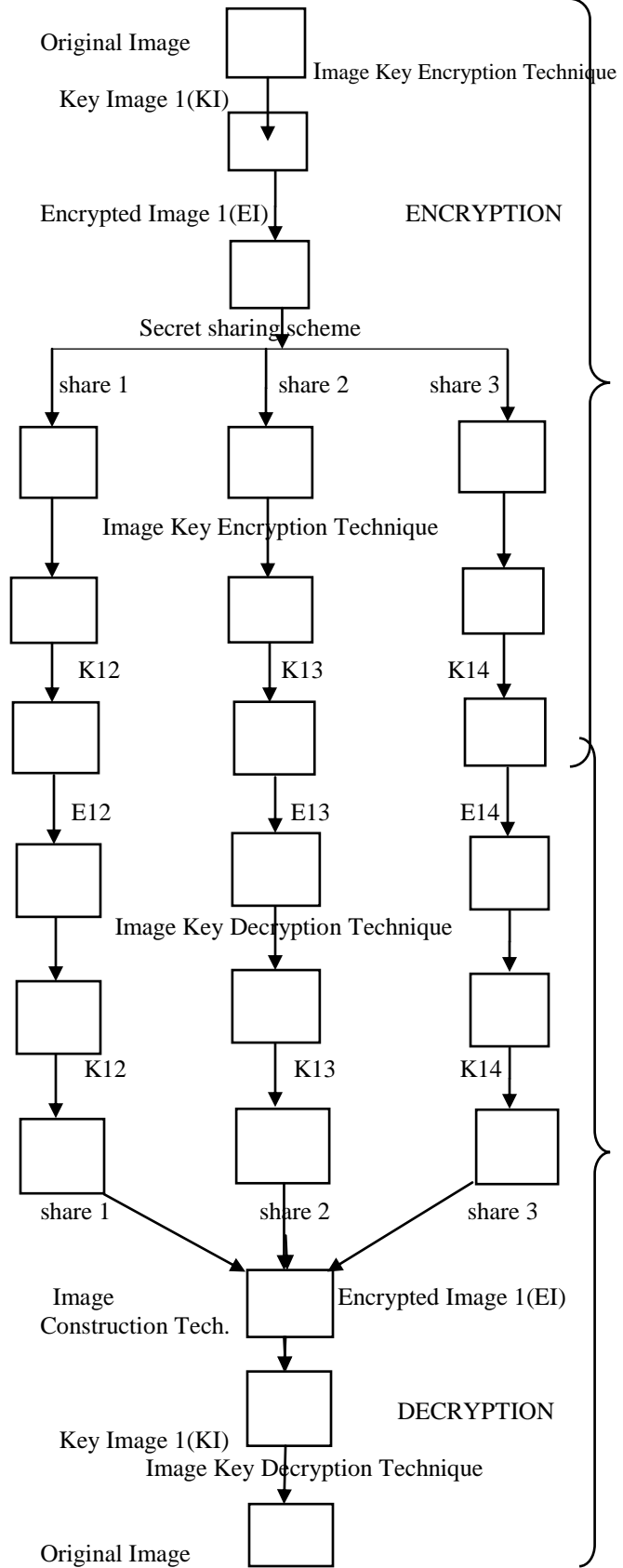


Figure 2. Diagrammatic representation of BWM&AS operation

III. OVERALL PROCEDURE

Step 1: In the proposed encryption technique where the original image is encrypted by using an image key.
 Step 2: Then divide encrypted image into N number of shares.
 Step 3: Each of the shares is again being encrypted by unique image keys in encryption end.
 Step 4: In decryption end retrieve original shares from the encrypted shares using appropriate image key and generate original encrypted image by taking K number of shares out of N.
 Step 5: Lastly retrieve the original image by performing user define operation between the original image key and encrypted Image. Figure 3 represents the overall procedure.



K12, K13, K14 are Key Images and E12, E13, E14 are Encrypted Image Shares.

Figure 3. Block diagram of the overall procedure for proposed technique.

IV. ENCRYPTION PROCESS

A. Procedures for Encryptions

1) Image key encryption algorithm (IKE algorithm)

Step I: Take an image as input and calculate its width (w) and height (h).

Step II: Create an array IMG_ORG of size $w \times h \times 32$ to store the binary pixel values of the image using the following loop.

```
For i = 0 to (w*h-1)
{ Scan each pixel value of the image and convert it into
32 bit binary string called PIX.
for j = 0 to 31
{ IMG_ORG [i*32+j] = PIX.charAt(j).
}}
```

Step III: Create an array IMG_RGB of size $w \times h \times 24$ to store the binary values of only 24 bit RGB part of the source image using the loop.

```
For i = 0 to (w*h-1)
{ Construct a 24 bit string SUB_PIX from 32 bit PIX
string rejecting the 8 bit alpha part by
SUB_PIX=PIX.substring(8, 32).
for j = 0 to 23
{ IMG_RGB [i*24+j] = SUB_PIX.charAt(j).
}}
```

Step IV: Take an image as secret image key and calculate its width (wk) and height (hk). Where the condition $wk < w$ and $hk < h$ must satisfy.

Step V: Create an array IMG_KEY of size $wk \times hk \times 24$ to store the binary pixel values of the image using the loop.

```
For i = 0 to (wk*hk-1)
{ Scan each pixel value of the image and convert it into 32
bit binary string let PIX_KEY.
Construct a 24 bit string SUB_PIX_KEY from 32 bit
PIX_KEY string rejecting the 8 bit alpha part by
SUB_PIX_KEY = PIX_KEY.substring(8, 32).
for j = 0 to 23
{IMG_KEY[i*24+j] = SUB_PIX_KEY.charAt(j).
} }
```

Step VI: Assign the bit length of IMG_KEY, $wk \times hk \times 24$ to LEN.

Calculate $DIV = (w \times h \times 24) / LEN$. DIV determines the number of times key image fully covers the original image. Calculate the remainder portion $REM = (w \times h \times 24) \% LEN$. REM determines the number of pixels of original image is left to be covered.

BWM&AS is performed between IMG_KEY array and IMG_RGB array by the following process.

For i = 0 to (DIV-1)

```
{ for j = 0 to (LEN -1) {
```

```
IMG_RGB[i*LEN+j] = IMG_RGB[i*LEN+j] (BWM&AS
OPERATION) IMG_KEY[j].
```

```
} }
```

For i = 0 to (REM-1){

```
IMG_RGB [DIV*LEN+i] = IMG_RGB [DIV*LEN+i]
(BWM&AS OPERATION) IMG_KEY[i].
```

```
}
```

Step VII: Replace only RGB portion of IMG_ORG [$w \times h \times 32$] with the BWM&AS ed RGB value of IMG_RGB [$w \times h \times 24$]. So that, alpha part remains unchanged. It is done by following loop

For i = 0 to (w*h-1){

```
for j = 0 to 23 {
```

```
IMG_ORG [i*32+j+8] = IMG_RGB [i*24+j].
```

```
}}
```

Step VIII: create a one dimensional array IMG_CON [$w \times h$] to store constructed pixel values. Construct Alpha, Red, Green and Blue part of each pixel by taking consecutive 8 bit substring starting from 0th bit. Construct pixel from these part and store it into IMG_CON [$w \times h$].

Step IX: Generate image IMG_ENCRYPT from IMG_CON [$w \times h$].

2) Secret sharing encryption algorithm (SSE algorithm)

Step I: Take an image as input and calculate its width (w) and height (h).

Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image. k must be less than or equal to n.

Step III: Calculate $recons = (n - k) + 1$.

Step IV: Create a three dimensional array $img_share[n][w*h][32]$ to store the pixels of n number of shares.

```

Step V: for i=0 to (w*h-1)
{Scan each pixel value of the image and convert it into 32
bit binary string let PIX.
For j=0 to 31
{ if ith position of PIX contains '1'
Call Random_Place(n, recons).
for k=0 to (recons-1) {Set  $img\_share[rand[k]][i][j] = 1$ .
}}

```

Step VI: Create a one dimensional array $img_cons[n]$ to store constructed pixels of each share.

```

Step VII:
for k1=0 to (n-1){for k2=0 to (w*h-1){ String value= ""}.
for k3=0 to 31 {value=value+ $img\_share[k1][k2][k3]$ }.
construct alpha, red, green and blue part of each pixel by
taking consecutive 8 bit substring starting from 0.
construct pixel from these part and store it into
 $img\_cons[k1]$ }.
generate image from  $img\_cons[k1]$ }.

```

```

Subroutine int Random_Place (n, recons)
{ create an array rand [recons] to store the random number
generated.
For i=0 to (recons-1)
{generate a random number within n, let rand_int.
If (rand_int is not in rand[recons])
rand[i] = rand_int}.
return rand[recons]}.

```

3) Encryption algorithm for proposed process

- Take two images as inputs: Original image and Key image.
- Use IKE algorithm one time to obtain an encrypted image.
- Take the encrypted image as input.
- Use SSE algorithm to obtain n number of shares from the encrypted input image.
- Take each share and unique image keys for each share as inputs.
- Use IKE algorithm n times to obtain n number of encrypted image shares.

V. DECRYPTION PROCESS

A. Procedures for Decryptions

The decryption is done by two steps. First sufficient numbers (k) of shares are collected and bitwise OR operation is performed among those to reconstruct the encrypted image. Secondly decryption is performed on the

revealed encrypted image by the key to generate the original image. The algorithms used for decryption are described in the following section.

1) Image key decryption algorithm (IKD algorithm)

Step I: Let the revealed encrypted image is taken as input.

Step II: The image key is taken as input.

Step III: Follow the algorithm for BWM&AS operation to generate the original image.

[As A BWM&AS B = C then C BWM&AS B = A].

2) Secret sharing decryption algorithm (SSD algorithm)

Step I: Input number of shares to be taken (k), height (h) and width (w) of each share.

Step II: Create a two dimensional array $share[k][w*h]$ to store the pixel values of each share. Create a one dimensional array $final[w*h]$ to store the final pixel values of the image to be produced by performing OR operation.

```

Step III: For i=0 to k-1
{input the name of the ith image share to be taken.
for j=0 to (w*h-1){Scan each pixel value of the ith image
share and store the value in  $share[i][j]$ .
}}

```

```

Step IV: For i=0 to (k-1) {for j=0 to (w*h - 1){
 $final[j]=final[j] | share[i][j]$ ; [ | is bitwise OR]
}}

```

Step V: Generate image from $final[w*h]$.

3) Decryption algorithm for proposed process




- Take encrypted shares and corresponding unique image keys that were used in Encryption Algorithm for proposed process in step 3(i) as inputs.
- Use IKD algorithm n times to obtain n number of decrypted image shares
- Take decrypted k number of shares from n number of shares as input.
- Use SSD algorithm to construct a decrypted image.
- Take the decrypted image and the key image (i.e., the image key that we used in Encryption Algorithm for Proposed Process step 1).
- Use IKD algorithm to retrieve the Original image.

VI. EXPERIMENTAL RESULT & DISCUSSION

A. Encryption Process

Level-1: Encryption using image key & BWM&AS operation.

Figure 4, Figure 5 and Figure 6 represents original image, key image and encrypted image respectively.

parrot.png	pikachu.jpg	Encrypted1.png
		
Figure 4. Original Image.	Figure 5. Key Image1.	Figure 6. Encrypted Image1.

Level-2: Encryption using secret sharing scheme and image key encryption technique using BWM&AS operation.

a) *k-n Secret Sharing Scheme:*

Name of the Inputted image: Encrypted1.png.

Number of Shares (N): 4

Numbers of shares to be taken (K): 3

Figure 7 represents all image shares produced after applying Secret Sharing Scheme.





	
0img.png	1img.png
	
2img.png	3img.png

Figure 7. Image shares produced from k-n secret sharing.

b) *Image key encryption applied on each share:*

Figure 8 represents all the image shares and their corresponding key images and encrypted shares.



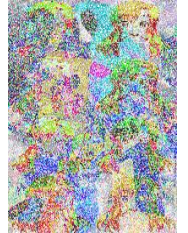


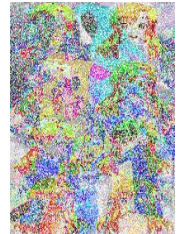

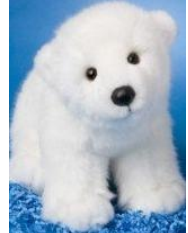
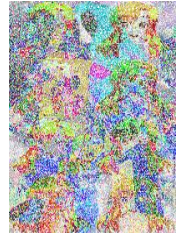


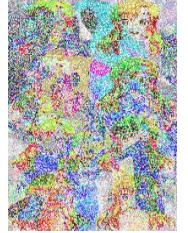
Image Shares	Key images	Encrypted Shares
		
0img.png	kitty.jpg	Encrypted2.png
		
1img.png	pinkpost.jpg	Encrypted3.png
		
2img.png	shiver.jpg	Encrypted4.png
		
3img.png	tulip.jpg	Encrypted5.png

Figure 8. Encryption of image shares using image keys.

B. Decryption Process

Level-1: Decryption using secret sharing scheme and image key encryption technique using BWM&AS operation.

a) *Decryption of shares applying image key*

Figure 9 represents all the encrypted shares and their corresponding key images and decrypted shares.

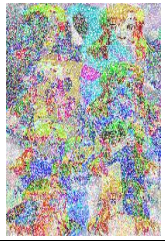






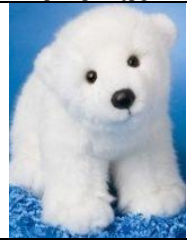




Encrypted Shares	Key images	Decrypted Shares
		
Encrypted2.png	kitty.jpg	0img.png
		
Encrypted3.png	pinkpost.jpg	1img.png
		
Encrypted4.png	shiver.jpg	2img.png
		
Encrypted5.png	tulip.jpg	3img.png

Figure 9. Decryption of image shares using image keys.

b) Reconstructing of encrypted image from shares

Number of shares to be taken: 3
 Height and Width of each share: 200, 200
 Shares inputted: 0img.png, 1img.png, 3img.png.




Figure 10 represents the reconstructed encrypted image.



Figure 10. Reconstructed encrypted image

Level-2: Decryption using image key & BWM&AS operation.

Figure 11, Figure 12 and Figure 13 represents reconstructed encrypted image, key image and original image respectively

Reconstructed encrypted image	pikachu.jpg	parrot.png
		
Figure 11. Reconstructed encrypted Image	Figure 12. Key Image1	Figure 13. Original image

VII. CONCLUSION

Here we proposed a private-key image encryption scheme based on bit wise masking and alternate sequence (BWM&AS) operation between two constitutive bits of each pixel of original image and image key (image key encryption technique) followed by the secret sharing scheme to generate multiple number of shares where each share is being encrypted by the user defined image keys.

As three level of encryptions are being combined together for the proposed system, so the security is increased.

We introduce a new operation BWM&AS for the first time where multiple number of micro operations are being combined together to generate the entire operation Thus the security is increased in a great entrance.

In the proposed system, information about specified K numbers of encrypted shares, all image keys and proper mapping information between the encrypted image and the keys can break the security of the system, but all these information are being hidden and changed as per the user choice. Thus enhance the security of the proposed system.

All the inputted image keys are user defined so the variability of size, type and dimension of the image key file are being defined by the user which imposes a better security on the system.

Besides this, a user can also do the encryption of an inputted image by using several numbers of distinct image keys where each key is allotted for a specific block among

several numbers of user-defined blocks in a inputted image file. So the security is increased.

The execution time is depends on the file size not on the type of the file as we have done the encryption in bit level.

The only drawback is that if the value of the N (number of share to be converted) is very higher then it will take very much time to generate all N numbers of shares. Thus the encryption or decryption time will be increased.

REFERENCES

- [1] M. AL-Laham Mohamad, "Encryption-decryption RGB color image using matrix multiplication", International Journal of Computer Science & Information Technology (IJCSIT), Vol. 7, No 5, October 2015.
- [2] Saksham Wason, Piyush Kumar and Shubham Rathi, "Text and image encryption using color image as a key", International Journal of Innovative Research in Technology (IJIRT), 2014.
- [3] R. Das, S. Kulia, S. Dutta, "An Approach Of Visual Cryptography Scheme For Color Image By Cumulative Encryption Using Image Partitioning, Text Key Encryption, Image Key Encryption & Digital Enveloping", International Journal of Engineering Research & Technology, Volume 2, Issue 5, PP-1341-1349, 2013.
- [4] A. Bhakta, S. Maity, R. Das, S. Dutta, "An Approach of Visual Cryptography Scheme by Cumulative Image Encryption Technique Using Image-key Encryption, Bit-Sieved Operation and K-N Secret Sharing Scheme.", International Journal of Innovative Technology and Exploring Engineering (IJITEE), www.ijitee.org (ISSN: 2278-3075, Vol. 3 Issue 1.), pp 20-23 June-2013.
- [5] S. Kandar, B.C Dhara., "Random sequence based secret sharing of an encrypted color image", RAIT, 2012, ISM Dhanbad, INDIA.
- [6] S.M.M.Karim, Md. S. Rahaman, Md. I. Hossain, "A new approach for LSB based image steganography using secret key," **IEEE Xplore**, DOI: 10.1109/ICCITechn.2011.6164800, Bangladesh, March, 2012. [Computer and Information Technology (ICCIT), Bangladesh, 2011].
- [7] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, PP- 1-12, 1995.
- [8] Ranjan Parekh, "Principles of Multimedia", Tata McGraw Hill, INDIA, 2006.
- [9] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications", Cambridge University Press, 2009.
- [10] Digital content for steganography, link" www.garykessler.net/library/steganography.html".

Authors Profile

Mr. Ramkrishna Das has achieved MBA, M.Tech (C.S.E.), MCA degree and currently pursuing PhD from Vidyasagar University. He has working experience over 9 years as Assistant Professor in Haldia Institute of Technology and 2 years as Teacher. Government Administrative



Officer. Currently he is working as Development Officer in Bankura University, INDIA. He has published 3 books from international publisher including Lambert Academic Publishing, GERMANY. He has published 20 numbers of research articles in international journals (including Scopus and UGC indexed journals) and conferences (including IEEE and Springer conferences).

Dr. Saurbh Dutta pursued Ph. D. (Computer Science), MCA, B. Sc. (Mathematics). His publications, experiences and achievements are furnished below: Publication of book- 2.



Research papers publications:43, Foreign Journal Publications - 11 Peer-Reviewed International Conference Papers - 8, Indian Journal Publications - 2, Published/Accepted in International Conference -7, others - 3.National Conference Publications -12.

Research experience- 14 years. Specialization: Information Security and Cryptology. Membership -IACSIT, IJIST, IEDRC, , IJISMARD, IJMCAR, IJCSS, IJMER, ISOC, IAENG, IJCSI. Reviewer-(IJNS), Taiwan AMSE, France, IJACSA, ICCIA, ACCT12. Award- Enlisted in the directory of Marquis Who's Who in the World in its 2010 edition. Biography selected for inclusion by ABI (American Biographical Institute, Inc.) in the list of International Profiles of Accomplished Leaders in its 2011 edition.